Vorwort des Herausgebers

In der digitalen Welt existieren nur digitale Identitäten. Diese auf reale Menschen „aus Fleisch und Blut“ zu beziehen, ist eine zentrale Herausforderung der digitalen Welt. Zwischen der digitalen Identität und der real existierenden Person gibt es keine unmittelbare Verbindung. Daher kann eine Person mehrere digitale Identitäten haben, kann eine digitale Identität ohne Bezug zu einer Person bestehen und können digitale Identitäten „gestohlen“ werden. Digital können bestimmte Merkmale einer Person erfasst werden – ob diese ihre Identität „ausmachen“, eine bestimmte real existierende Person beschreiben oder in der Anonymität aller Merkmalsträger „untergehen“ lässt, kann immer umstritten sein.

Vielfach muss jedoch für digitales Handeln klar, oft sogar eindeutig sein, welche reale Person durch eine digitale Identität vertreten wird. E-Business funktioniert nur, wenn die handelnden Personen bekannt und eindeutig über ihre digitale Identität bestimmbar sind. Nur dann können Willenserklärungen ihnen zugeordnet werden, für sie Rechte und Pflichten begründen und diese notfalls durchgesetzt werden. E-Commerce funktioniert nur, wenn ausreichend bestimmt ist, wer als Käufer und wer als Verkäufer auftritt. E-Government erfordert eine ausreichende Identifizierung der Behörde, des handelnden Verwaltungsbeamten und des Bürgers als Antragsteller oder als Adressat von Verwaltungshandeln. E-Justice setzt voraus, dass Kläger, Beklagter und Gericht ausreichend bekannt sind und identifiziert werden können. Um ein letztes Beispiel der E-Welten zu wählen: Für E-Health müssen Arzt und Patient ausreichend identifiziert sein, um Vertrauen und Verantwortung zu begründen und einzufordern. Alle diese Beispiele zeigen, dass das Verwalten von digitalen Identitäten und die Sicherung ihres Bezugs zu realen Personen nicht nur wichtig für einzelne Gesellschaftsbereiche, sondern eine Basisfunktionalität moderner Gesellschaften sind.

Was „ausreichend bestimmt“ und was „Identität“ heißt, ist von Bereich zu Bereich unterschiedlich. Im einen Fall sind Name und Anschrift, im anderen Fall ist eine Identifikationsnummer und im dritten Fall ein Set persönlicher Merkmale erforderlich. Wie verlässlich eine digitale Identität und wie belastbar der Bezug zu einer real existierenden Person sein müssen, hängt von den Funktionsanforderungen des jeweiligen Gesellschafts-

bereichs ab. Dieser entscheidet auch darüber, wieviel Identifikation erforderlich ist, wieviel informationelle Selbstbestimmung in der Bekanntgabe von Identifikationsdaten zum Ausdruck kommen kann und wieviel anonymes Handeln ohne Identifizierung möglich ist.

Wie der Bezug zwischen einer digitalen Identität und einer real existierenden Person hergestellt und gesichert wird und wie er verschleiert, unterbrochen oder verhindert werden kann, hängt auch ab von den technisch-organisatorischen Möglichkeiten. Er kann gesichert werden durch Kennziffern, Speicherorte, Zugriffsrechte, Merkmale technischer Geräte, Token, Wissensmerkmale, biometrische Merkmale, digitale Zertifikate, Signaturen, Siegel und Zeitstempel. In anderen Situationen können Credentials oder Pseudonyme ausreichen. Wieder in anderen Situationen kann oder muss anonymes Handeln – gesichert durch Anonymisierungsdienste – akzeptiert werden.

Die technischen, rechtlichen und ökonomischen Rahmenbedingungen, die über die Nutzung dieser vielfältigen Möglichkeiten, Personen digital zu identifizieren und zu anonymisieren, entscheiden, haben sich mit der Entwicklung von Staat und Wirtschaft immer wieder verändert und werden auch künftig die Entwicklung digitaler Identitäten bestimmen. Der historische Blick auf das Phänomen kann hinsichtlich der Abhängigkeiten das Verständnis für die heutigen Probleme schärfen.

Die aktuelle Situation ist geprägt von zwei Polen. Auf der einen Seite stehen private, sektorielle und technisch sehr unterschiedlich sichere (und datenschutzfreundliche) Lösungen, die zumindest in solchen Bereichen Verbreitung erlangen, in denen es nicht auf „starke“ Rechtswirkungen ankommt. Auf der anderen Seite versuchen staatliche Stellen auf unterschiedlichen Ebenen seit Jahren, rechtlich hoch durchstrukturierte und technisch komplexe Basisfunktionalitäten zu etablieren, denen Rechtswirkungen zugesprochen werden (zuletzt mit der eIDAS-VO). Bisher ist keine Seite wirklich erfolgreich – aus Gründen der technischen Komplexität, fehlender Geschäftsmodelle und hoher Benutzerunfreundlichkeit.

In dieser Situation besteht Bedarf nach einer Bestandsaufnahme, die Begriffe und Entwicklungen darstellt, Rahmenbedingungen klärt und Entwicklungsperspektiven aufzeigt. Dieser Aufgabe hat sich das von Prof. Dr. Gerrit Hornung geleitete, durch die Deutsche Forschungsgemeinschaft (DFG) geförderte wissenschaftliche Netzwerk „Der digitale Bürger und seine Identität“ während seiner dreijährigen Laufzeit gewidmet. Die in diesem Band dokumentierten Ergebnisse bieten einen Überblick zum Phänomen der digitalen Identität, entwickeln theoretische Erkenntisperspekti-

ven, vertiefen wichtige aktuelle Fragen und zeigen Lösungswege für die weitere praktische Entwicklung auf. Angesichts der noch zunehmenden Bedeutung des elektronischen Identitätsmanagements für eine sichere, effiziente und datenschutzfreundliche Abwicklung elektronischer Rechts- und Geschäftsprozesse ist dem Werk zu wünschen, dass es sowohl in der Wissenschaft als auch bei den Entscheidern in Politik, Verwaltung und Wirtschaft entsprechende Beachtung findet.

Kassel, im Mai 2016 *Alexander Roßnagel*

Inhalt

Einleitung

Gerrit Hornung / Christoph Engemann

1 Identität – von der Unmöglichkeit einer Definition

„Identität“ ist ein in seiner Vielschichtigkeit zugleich starker und schwacher Begriff. Er entwickelt seine Stärke, wo er entweder einzelne wissenschaftliche Theorien begrifflich fokussiert oder Konzepte verschiedener Wissenschaftsdisziplinen verbindet und so füreinander anschlussfähig macht. Diese Offenheit des Begriffs ist zugleich seine Schwäche: Identität kann alles, und damit am Ende nichts bedeuten. In seiner Konturenlosigkeit liegt die Gefahr, nichts Bestimmtes mehr zu bezeichnen und damit letztlich gar kein Begriff mehr zu sein. Die Verwendung des Worts birgt deshalb das Risiko von Missverständnissen und wissenschaftlichen Diskussionen, bei denen die Teilnehmer nur meinen, über dasselbe zu sprechen.

Eine Lösung kann nicht darin bestehen, den Begriff prinzipiell definitorisch zu verengen, weil er dann zugleich seine Stärke verlieren würde. Stattdessen muss die Unschärfe offengelegt und produktiv genutzt werden: Eine gelungene Mischung aus Prägnanz und Assoziationskraft lässt sich erzielen, wenn man den Identitätsbegriff kontextbezogen definiert, zugleich aber für angrenzende, oftmals befruchtende Konzepte offen hält. Dies ist ein wesentliches Ergebnis des durch die Deutsche Forschungsgemeinschaft (DFG) geförderten wissenschaftlichen Netzwerks „Der digitale Bürger und seine Identität“, aus dem der vorliegende Band entstanden ist. Wer dementsprechend in dieser Einleitung eine für das gesamte Werk gültige Definition von Identität oder digitaler Identität erwartet, muss enttäuscht werden, sollte diese Enttäuschung aber gerade als Ansporn begreifen, von der eigenen wissenschaftlichen Warte aus nach anschlussfähigen Konzepten zu suchen und diese in Auseinandersetzung mit anderen Konzepten fortzuentwickeln.

Den Hintergrund der folgenden Untersuchungen bilden die vernetzten Welten des Internets, in denen Bürger eine „digitale Identität“ ausbilden. Der Begriff des Bürgers verweist auf die Zugehörigkeit zu einer staatlich verfassten Gemeinschaft, das Possessivpronomen „seine“ zudem auf den

Anspruch, Anteil an dem zu haben, was in dieser Gemeinschaft als die je eigene Identität gelten soll. Als digitale ist diese Form von Identität eine Teilmenge des allgemeinen Identitätsbegriffs, erweitert diesen aber zugleich. Auch der Begriff des Digitalen kann eng (im Sinne diskreter Signale) oder weit (digitale Technologien und Medien und das Handeln mit ihrer Hilfe) verwendet werden. Dementsprechend werden unterschiedliche Wissenschaften mit digitaler Identität Unterschiedliches verbinden. In jedem Fall entsteht diese aber, wo soziales Handeln und digitale Medien aufeinander treffen, insbesondere im alltäglichen Beispiel kommunikativer Handlungen in Online-Kontexten. In diesen Handlungen gibt der Einzelne Informationen über sich preis oder verweigert diese Preisgabe. Spiegelbildlich sammeln viele andere Akteure (private Kommunikationspartner, Unternehmen, Behörden) Informationen über die Nutzer, speichern oder löschen diese, behalten sie für sich oder geben sie an andere weiter. An diesen Prozessen von digitaler Identitätsstiftung sind die Betroffenen in unterschiedlichem Maße aktiv und passiv beteiligt.

2 Identität, Anonymität und Pseudonymität

Im Internet sind die Nutzer als Individuen teilweise von Anfang an oder zu einem späteren Zeitpunkt erkennbar, teilweise bleiben sie für alle oder doch für manche Kommunikationspartner im Verborgenen. Digitale Identität steht deshalb in einem unauflöslichen Zusammenhang mit den Phänomenen der Anonymität und Pseudonymität. Aufgeworfen ist damit die Frage nach den Verfahren und Regelungen, die es ähnlich wie Namen und Adressen im analogen Raum erlauben, Menschen zuverlässig und über Zeit zu adressieren. Während die ikonische, 1993 in der Zeitschrift New Yorker veröffentlichte Karikatur Peter Steiners „On the Internet, nobody knows you are a dog“ noch die spielerische Seite dieses Themas beleuchtete, werden die zugrundeliegenden Konflikte seit einiger Zeit mit erheblicher Vehemenz ausgetragen. Bürgerrechtler und viele Politiker, aber auch Hacker und Gruppen wie Anonymous sehen anonymes Handeln im Internet als unabdingbar für individuelle Persönlichkeitsentfaltung und offenen Meinungsaustausch an und damit für demokratische Gesellschaften als solche. Dagegen lassen sich vor allem von staatlicher Seite immer wieder Stimmen vernehmen, die solches mit dem Internet einhergehende Unwissen nicht akzeptieren wollen. Auch dort müsse es Möglichkeiten zur eindeutigen Identifikation von Menschen geben. Autokratische Staaten wie

China, Russland und der Iran versuchen inzwischen Klarnamenregelungen für das Internet durchzusetzen. In liberalen Demokratien wird um die Form, Reichweite und Kontrolle von digitalen Identifikationsmechanismen intensiv gestritten. Die digitale Ökonomie hat derweil das Auswerten von Daten längst zu ihrer Geschäftsgrundlage gemacht und schafft für die Formen und Kontrolle individueller Selbstrepräsentation eigene und wirkmächtige Realitäten. Identität, so zeigt bereits diese kursorische Aufzählung, ist nicht einfach da, sondern ein Konstrukt, das unter den Bedingungen des digitalen Wandels besonders prekär geworden ist.

Jenseits theoretischer Fragen nach analoger und digitaler Identität finden sich inzwischen vielfältige Beispiele aus der Praxis, die durch unterschiedliche staatliche und private „Identitätsprovider" organisiert und angeboten werden. Von der breiteren Öffentlichkeit wenig beachtet und kaum genutzt, hat Deutschland in den letzten 20 Jahren eine ganze Reihe von ambitionierten Großprojekten zur Bereitstellung digitaler Identitäten initiiert und implementiert. Gemeinsam ist diesen Projekten, denen auch das Hauptaugenmerk des wissenschaftlichen Netzwerks galt, dass sie dem Bürger nicht mehrere, sondern eine einzelne und der Person eindeutig zugehörige Identität zuordnen sollen. Dazu zählen mit dem neuen Personalausweis und der elektronischen Gesundheitskarte Chipkarten, die sich bereits in vielen Geldbörsen finden, aber bei den Bürgern bisher wenig Akzeptanz und Anwendung erfahren.

Für die meisten Bürger ist es im selben Zeitraum vielmehr selbstverständlich geworden, mehrere digitale Identitäten in verschiedenen Diensten wie Facebook, Gmail, Amazon oder XING zu unterhalten. Eine vom Staat mittels Chips auf Personalausweisen oder Gesundheitskarten bereitgestellte Identität erscheint hier zunächst als eine zusätzliche unter vielen, deren Nutzen zudem nicht unmittelbar evident ist. Demgegenüber begreifen Gesetzgeber und Verwaltung diese Angebote als essentielle Bestandteile der Sicherheit des elektronischen Rechtsverkehrs, der Gewährleistung von Datenschutz und der Vereinfachung von Verwaltungsverfahren durch die Bereitstellung staatlicher Leistungen im Internet. Die digitale Identität steht so im Konfliktfeld zwischen staatlichen Gestaltungsbegehren, tatsächlichen Nutzungsformen und politischen Fragen nach den gesellschaftlichen Zuständigkeiten des digitalen Wandels. Der vorliegende Band möchte diese Fragen aus verschiedenen Blickwinkeln analysieren, aber auch der interessierten Öffentlichkeit einen vertiefenden Einblick in die entsprechenden Hintergründe, Konfliktlinien und gegenwärtigen Entwicklungen geben.

3 Konstruktion, Herstellung und Gestaltung digitaler Identität – die Rolle des Staates

Vor dem Hintergrund der jüngeren Entwicklungen sowohl in Europa als auch in den USA ist davon auszugehen, dass staatlichen Akteuren bei der Gestaltung der digitalen Identität eine größere Rolle als bisher zukommen wird. Wie die hier versammelten Beiträge zeigen, erweist sich digitale Identität als komplexes Ensemble aus rechtlichen, ökonomischen, sozio-technischen und medialen Aspekten, deren Konturen keineswegs fest stehen, sondern vielmehr äußerst konflikthaft sind. Ein wesentlicher Grund liegt in dem Charakter des Internets als einem transnationalen Medium, das insbesondere in Bezug auf die Nutzer und deren Präferenzen und Verhalten besonders stark von Marktkräften geprägt ist. Staatliche Akteure haben das Internet historisch zwar auf den Weg gebracht, sind aber seit den neunziger Jahren des vorigen Jahrhunderts bei seiner Gestaltung und vor allem bei der Entstehung neuer Nutzungsformen in den Hintergrund getreten. Mit der Verbreitung staatlich regulierter Infrastrukturen des Electronic Government, aber auch mit dem zunehmenden sicherheitsbehördlichen Streben nach weitreichenden Datensammlungen scheint sich hier ein Wandel anzubahnen.

Für die wissenschaftliche und politische Analyse muss man sich bewusst machen, dass Identität, Anonymität, Pseudonymität und verwandte Phänomene nicht einfach existieren, sondern geschafften werden (müssen) – ob mit oder ohne staatliche Beteiligung. Macht der Staat, wie bei der Entwicklung und Implementierung des neuen Personalausweises, Vorgaben, so schließt dies häufig an bereits existierende und in vielfältige Prozesse eingebundene Identitätsmedien an. So hat die personale Identität rechtliche und technische Voraussetzungen: Sie rekurriert auf Namen, auf Bilder und Unterschriften, auf Ausweise und Urkunden und auf die entsprechenden gesetzlichen Normen, die sich vor allem im Personenstands-, Melde-, Pass- und Personalausweisrecht, aber auch in vielen, teils verstreuten Bestimmungen über Formvorschriften, Beweiswert und Identifizierungsanforderungen finden.

Diese Normen enthalten Regelungen und Verfahren, die im analogen Raum kaum noch besondere Aufmerksamkeit erfahren und oft selbstverständlich erscheinen. Mit der Digitalisierung werden Verfahren wie die Unterschrift oder die gegen Einblicke geschützte Übermittlung eines Dokuments aber wieder und teilweise in gänzlich neuer Weise problematisch. Was eine Person ist, wie sie als solche adressiert werden und andere adres-

sieren kann, erweist sich als komplexer Prozess, bei dem Marktkräfte mit rechtlichen, technisch-infrastrukturellen und medialen Prozesse in vielfacher Weise interagieren, ineinandergreifen oder im Widerstreit liegen. Für welche digitale Identitäten sich die Bürger entscheiden können oder müssen, welche dieser Identitäten in bestimmten Kommunikationsbeziehungen akzeptiert werden und wie das datenschutzrechtlich komplexe Verhältnis zwischen Identifizierbarkeit und Anonymität in der Praxis konstruiert wird, hängt von der weiteren Entwicklung dieser Prozesse ab.

Alle diese Dimensionen sind folglich gestaltbar. Gestaltungsprozesse benötigen wissenschaftlich fundierte Gestaltungskriterien und begleitende Analysen über Wirkkräfte, Akteure, Erfolge, Misserfolge und absehbare künftige Probleme. Die in diesem Buch versammelten Beiträge untersuchen die Lösungsversuche, die unternommen worden sind und gerade unternommen werden, um sich den Problemen der personellen Identität und der Anonymität im Internet zu stellen. Hierzu bedarf es neben konkreten Analysen einzelner Identitätslösungen auch der historischen und globalen Einordnung.

Vor diesem Hintergrund ergeben sich unterschiedliche Perspektiven auf eine inzwischen beinahe zwanzigjährige, konfliktreiche Geschichte vielfältiger Versuche, durch technische, wirtschaftliche und/oder rechtliche Mechanismen einen Ausgleich zwischen den verschiedenen legitimen Bedürfnissen von Bürgern, Wirtschaft und Staat zu erzielen. Diese Geschichte ist keineswegs abgeschlossen, sondern im vollen Gange. Die hier vorgestellten Beiträge verstehen sich deshalb auch als Bestandsaufnahme und Kommentar für die weitere Diskussion, die mit der neuen EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (so genannte eIDAS-Verordnung) und dem Prozess einer „National Strategy for trusted Identities in Cyberspace“ (NSTIC) in den USA auf der politischen Agenda nach oben gerückt ist.

4 Zu den Beiträgen dieses Bandes

Vor dem Hintergrund aktueller Erkenntnisse über die Datensammlungen von Nachrichtendiensten fragt *Christoph Engemann* nach den Möglichkeiten und Grenzen einer selbstbestimmten „Digitalen Identität nach Snowden“ und stellt die historische und aktuelle Entwicklung von staatlichen Identitätsregimes dar. Dabei wird zunächst ein Überblick der historischen Entwicklungen gegeben, die scheinbar selbstverständliche Aspekte der

personellen Identität wie lebenslang stabile Namen nach dem Vorname-Nachname Format, Geburtsurkunden aber auch Identitätsmedien wie Pässe und Ausweise hervorgebracht haben. Die Entwicklung dieser im Wesentlichen auf Papier basierenden Identitätsmedien ist gleichlaufend mit derjenigen der modernen Staatlichkeit und wurde von dieser aus ordnungspolitischen, sozialstaatlichen und kolonialen Interessen betrieben. Vor diesem Hintergrund zeigt der Beitrag, wie mit dem Aufkommen des Internets diese historisch entstandenen und staatlicherseits monopolisierten Formate der Identitätsstiftung krisenhaft geworden sind. Die aktuelle Lage der Debatte um die digitale Identität ist geprägt durch die Versuche, diese Krise zu gestalten und zu bewältigen. Sie ist einerseits auf dem Wege der öffentlichen Deliberation um die Gestaltung hoheitlich vergebener digitaler Identitäten, wie beispielsweise des neuen Personalausweises, angegangen worden. Andererseits wurde sie, wie nach den Veröffentlichungen durch Edward Snowden sichtbar geworden ist, im Geheimen mit der Entwicklung und Eskalation von Überwachungstechniken beantwortet. Die sich ergebene offene Frage lautet, in welchem Verhältnis diese beiden Verfahrensweisen der staatlichen Identitätsstiftung im Internet zueinander stehen und in die zukünftige Gestaltung von digitalen Identitäten einfließen müssen.

Johannes Eichenhofer und *Christoph Gusy* beschreiben einen Trend weg von der digitalen Identität hin zur „Digitalen Identifizierung". Ausgehend von verschiedenen Anforderungen an die Identifizierung im Rechtssystem stellt die digitale Kommunikation über Distanz neue Herausforderungen an kommunikativ begründete und rechtlich strukturierte Nähebeziehungen. Drei Problemfelder lassen sich herausgreifen. Erstens eröffnet das Internet besondere Möglichkeiten der multivariablen Datennutzung: Daten werden aus ihrem Erhebungszusammenhang herausgelöst (dekontextualisiert) und in neue Verarbeitungszusammenhänge eingeführt (rekontextualisiert). Dies vermag zweitens Indiz- und Beweiswirkungen zu verschieben, weil der Betroffene keinen Einfluss auf die Rekontextualisierung nehmen kann. Drittens ergeben sich erhebliche Gefahren des Missbrauchs, wenn neue Kontexte mit beliebigen – legitimen oder illegitimen – neuen Verwendungszwecken verbunden sind. Zur rechtlichen Bewältigung stellt sich die Frage eines rechtlichen Distanzgebots, das sich in Limitierungsgebote für die Erhebung und Verwendung personenbezogener Daten umsetzen lässt. Derartige Gebote lassen sich in den Grundrechten finden – nicht nur, aber insbesondere im Recht auf informationelle Selbstbestimmung. Da Distanz zwar geboten ist, aber nicht absolut gesetzt werden

kann (Identifizierung bleibt ebenso erforderlich), sind Instrumente und Rechtsformen für die Identifizierung gerade unter den Bedingungen von Distanz zu entwickeln. Ob diese Herausforderung gelingt, entscheidet sich nicht mehr national, sondern europäisch und global.

„Technische Voraussetzungen elektronischer Identifikation" werden von *Lexi Pimenidis* erläutert. Er entfaltet zunächst aus technischer Sicht die für das Identitätsmanagement relevanten Begriffe, vor allem Anonymität, Pseudonymität und identifizierte Person. Daran schließt sich ein Überblick zu den informationstechnischen Grundlagen an, die die Basis für praktisch alle staatlichen oder privaten Identitätsmanagementsysteme bilden. Die Fragen der Identifizierung (Welche reale Person ist der Nutzer?), Authentifizierung (Welche der gespeicherten Identitäten entspricht dem Nutzer?) und Autorisierung (Was darf der Nutzer?) werden immer wieder neu aufgeworfen, und zu ihrer Beantwortung existieren verschiedene technisch-organisatorische Umsetzungsmodelle, die sich hinsichtlich der technischen Komplexität, der Benutzbarkeit für die Bürger und der datenschutzrechtlichen Bewertung unterscheiden. Viele dieser Modelle (beispielsweise die elektronische Signatur) basieren auf asymmetrischer Kryptographie und erfordern ein komplexes Schlüsselmanagement. Neben diesen meist standardisierten, teils auch regulierten Verfahren, die mit dem Wissen der Betroffenen durchgeführt werden, eröffnet sich ein weiter Bereich intransparenter technischer Möglichkeiten der Wiedererkennung. Dies betrifft zum einen die Verkettung von Informationen aus unterschiedlichen Kontexten (beispielsweise durch Cookies), zum anderen staatliche Datensammlungen wie die Vorratsdatenspeicherung. Beides reduziert die Möglichkeiten für anonymes Handeln signifikant, weil die verfügbaren Maßnahmen gegen Identifikation und Verkettung bisher noch mit starken Einschnitten in die Benutzbarkeit verbunden sind.

Jan Schallaböck geht von verschiedenen Identitätsbegriffen aus, schlägt eine relationale Variante zur Verständigung vor und erweitert die Perspektive auf das „Identitätsmanagement als Grundlage von Verhaltenssteuerung". Hierzu unterscheidet er auf Basis der Arbeiten des Europäischen Exzellenznetzwerks FIDIS drei Typen von Identitätsmanagement, nämlich Identitätsmanagementsysteme für das Management von (Benutzer)konten (Typ 1), Identitätsmanagementsysteme für das Profiling von Nutzerdaten durch eine Organisation (Typ 2) und Identitätsmanagementsysteme für nutzerkontrolliertes kontextabhängiges Rollen- und Pseudonymmanagement (Typ 3). Während für Typ 1 seit vielen Jahren Industriestandards verfügbar sind und Typ 2 in zahlreichen Implementierungen vorliegt, ist Typ

3 nicht nur theoretisch, sondern auch praktisch-technisch voraussetzungsvoll. Perspektivisch eröffnet er nicht nur den Anschluss an Konzepte der funktionalen Differenzierung und der kontextuellen Integrität, sondern auch die Aussicht einer erheblichen Ermächtigung des Nutzers zur Kontrolle über seine Daten. Wendet man die Typologie auf konkrete Profilingsysteme an, so wird der Umfang der Datensammlungen deutlich: Der Mensch wird als Kunde statistischen Vergleichsgruppen gegenübergestellt, mit gezielter Werbung adressiert und Scoringverfahren unterworfen. Er wird in seiner Alltagskommunikation in sozialen Netzwerken und E-Mail Diensten beobachtet und auf sein zu erwartendes Verhalten analysiert. Schließlich unterliegt er als potentieller Verdächtiger oder Störer neuen technischen Überwachungsinstrumenten wie der Deep Packet Inspection und modernen Mustererkennungsverfahren. Die Datenerhebung und statistische Einordnung wirft ungelöste datenschutzrechtliche Probleme auf.

Den auch von anderen aufgeworfenen Aspekt des „Unbemerkten Trackings im Internet" vertiefen *Dominik Herrmann* und *Hannes Federrath* und konstatieren als Ergebnis „Unsere unerwünschte Identität". Die Zeiten weitgehender Anonymität im Internet sind bis auf weiteres vorbei – nicht weil Nutzer bewusst und freiwillig erwünschte digitale Identitäten erzeugen, sondern weil Dritte ohne ihr Wissen unerwünschte digitale Identitäten miteinander verknüpfen. Wesentliches Motiv bildet die Möglichkeit, komplexe Online-Marketing-Systeme zu betreiben. Die zielgruppengenaue Präsentation von Werbung soll ihre Wirkung verbessern, aber auch und vor allem eine effektive Preisbildung für die Einblendung einzelner Anzeigen ermöglichen. Die dafür erforderliche Profilbildung birgt indes erhebliche Risiken: Manipulation der Wahrnehmung, Filter Bubble und Preisdiskriminierung. Die verwendeten Tracking-Techniken lassen sich in drei Kategorien einteilen, nämlich die gezielte Markierung von Endgeräten mittels Tracking-IDs (vor allem Cookies), das Auslesen technisch bedingter Eigenschaften der Endgeräte (aktives Fingerprinting, etwa von Browsern oder mittels System-IDs von Hardware) und das passive Tracking durch die Beobachtung des Datenverkehrs (Taktversatz der internen Systemuhr, verhaltensbasierte Verkettung etc.). In allen Bereichen existieren prinzipiell Gegenmaßnahmen, die aber mit praktischen Problemen zu kämpfen haben. Auch ergänzende Regulierungsbestrebungen wie die Do-not-track-Initiative oder die europäischen Cookie-Vorgaben erweisen sich als wenig effektiv. Folglich ergibt sich ein erheblicher Bedarf nach einem besseren Zusammenwirken zwischen Entwicklern und Regulierern.

In dem ersten von zwei Beiträgen zur internationalen Dimension digitaler Identität entfaltet *Gerrit Hornung* „Rechtliche Perspektiven des Identitätsmanagements in Europa“. Die Gründe für die Europäisierung der technischen, rechtlichen und sozialen Fragen des Identitätsmanagements liegen in der grenzüberschreitenden Natur von Internet-Infrastrukturen und in der Übernahme immer mehr kernstaatlicher Funktionen durch die Europäische Union. Diese bildet einen Harmonisierungsrahmen, der sich im globalen Kontext bislang nicht findet und der gegenüber privaten Angeboten den Vorzug rechtlicher Verbindlichkeit ermöglicht. Die Kompetenzen der Union zur Regulierung digitaler Identitäten haben sich erheblich erweitert. Mit der eIDAS-Verordnung bestehen nunmehr Vorgaben für die Erzeugung von Identitäten (Erstidentifizierung) und für ihre Verifikation, aber auch für verschiedene Sicherheitsniveaus der nationalen Vertrauensdienste und elektronischen Identifizierungsmittel. In den Bereichen der Interoperabilität, des Datenschutzes und des Verhältnisses zu Drittstaaten bestehen offene Fragen. Eine Analyse der europäischen Datenschutzreform offenbart ihre Auswirkungen auf das elektronische Identitätsmanagement insbesondere im Bereich des technischen Datenschutzes und der Zertifizierung. Als Herausforderungen für die Zukunft stellen sich die Ausfüllung des neuen rechtlichen Rahmens, die Zusammenarbeit über Europa hinaus und die kontinuierliche Entwicklung und Gestaltung datenschutzfreundlicher Technologien eines nutzerzentrierten Identitätsmanagements.

Jens Bender vertieft vor diesem Hintergrund „Technische Aspekte grenzüberschreitender Interoperabilität“. Die in den letzten 15 Jahren in vielen EU-Staaten eingeführten nationalen eID-Systeme unterscheiden sich technisch erheblich, beispielsweise durch den Einsatz von Chipkarten oder Passwörtern, die Verwendung oder den Verzicht auf einheitliche Personenkennzeichen und die Existenz oder das Fehlen zentraler Infrastrukturen. Wenn elektronische Identifizierungssysteme auch nicht die Identität, so doch eine (anwendungsabhängige) Menge von Identitätsattributen bereitstellen sollen, so müssen sie bestimmte Anforderungen erfüllen: Datenminimierung (Bereitstellung ausschließlich erforderlicher Attribute), nachweisbares Vertrauensniveau (technische und organisatorische Sicherheitseigenschaften) und gegenseitige Authentisierung (zwischen dem Besitzer der Identitätsdaten und dem Diensteanbieter, der diese erhalten möchte). Interoperabilität kann auf zwei Wegen erzeugt werden, nämlich im Gateway- und im Middleware-Modell. Ersteres setzt darauf, nicht die eID-Systeme selbst interoperabel zu machen, sondern Interoperabilität mittels Übersetzungsgateways zu erzielen, die zwischen dem nationalen eID-Sys-

tem des Identitätsinhabers und dem System des Empfängers der Identitätsdaten vermitteln. Im zweiten Ansatz erfolgt die Übersetzung zwischen verschiedenen eID-Systemen nicht durch zentrale Gateways, sondern durch eine (dezentral) beim Dienstanbieter installierte, standardisierte Middleware. Im Vergleich offenbart der Middleware-Ansatz zwar einen zusätzlichen Aufwand für die Diensteanbieter, reduziert jedoch denselben bei den Nutzern und erfordert keinen Aufbau zentraler – und damit sicherheitstechnisch wie datenschutzrechtlich problematischer – Instanzen.

Die internationalen Perspektiven digitaler Identität werden durch *Tile von Damm* auf „Die soziale Dimension von Privatheit und Identität in Indien" erweitert. Die sichere (digitale) Organisation zur eindeutigen Erkennung und Wiedererkennung der Mitglieder des Gemeinwesens ist auch in Indien eine zentrale Herausforderung, da die eindeutige Identifizierung einerseits Grundlage zahlreicher sozialstaatlicher Programme ist, andererseits Zugang zum Gemeinwesen verspricht. Tradierte religiöse und gesellschaftliche Gruppenzuordnungen in der indischen Gesellschaft (Kastensystem) erzeugen erhebliche Herausforderungen. Überdies fehlt es an Regelungen zu Privatheit und Datenschutz. Es existieren verschiedene Typen von Identitätspapieren, aber bis heute besitzt jeder vierte Bürger keinerlei derartige Dokumente. Das im Jahre 2009 gestartete Programm Aadhaar der Unique Identification Authority of India (UIDAI) hat das Ziel, die biometrischen und demographischen Angaben aller Einwohner zu erfassen und in einer zentralen Datenbank zu sammeln. In Kombination mit umfassenden Datenerhebungen im Bereich der Telekommunikation entstehen so Datensammlungen, die politischer und verfassungsrechtlicher Kritik ausgesetzt sind. Insgesamt ergibt sich ein Bild der immensen Herausforderungen für die Einführung digitaler Identitäten in Staaten, die große Modernisierungssprünge unternehmen, trotz vieler Bemühungen aber hohe Governancedefizite aufweisen und bisher keinen ausreichenden inklusiven Zugang für alle Bevölkerungsgruppen ermöglichen.

Zum Abschluss lenken *Heiko Roßnagel*, *Jan Zibuschka*, *Oliver Hinz* und *Jan Muntermann* den Blick auf die ökonomische Dimension der Verbreitung digitaler Identitäten, konkret die „Zahlungsbereitschaft für Föderiertes Identitätsmanagement". Bisherige Untersuchungen zum Erfolg und Misserfolg von Identitätsmanagementsystemen fokussieren auf die Angebotsperspektive. Die Autoren untersuchen demgegenüber – empirisch – die Nachfrageseite. Dabei wurden Probanden verschiedene Produkte zum Kauf angeboten, die sich in mehreren Faktoren unterschieden; möglich war auch der Verzicht auf einen Kauf. Die einzelnen Attribute betrafen die

Sicherheit (Bereitstellung der Attribute durch den Benutzer, Bereitstellung durch einen Dritten, zusätzliche Haftung des Dritten für die Angaben), den Datenschutz (Verwaltung aller Nutzerdaten durch einen Identitätsprovider als Treuhänder, Speicherung der Daten ausschließlich beim Nutzer mit Freigabe in jedem Einzelfall, Ermöglichung eines anonymen Attributsnachweises mittels anonymer Credentials), die Einsatzgebiete (ausschließlich nicht-kommerziell, nicht-kommerziell und kommerziell im E-Commerce, alle Web-basierten Dienste einschließlich E-Government) sowie den Preis (2, 5, 10, 20 und 40 Euro pro Jahr). Eine Analyse unter Berücksichtigung verschiedener Kundensegmente zeigt, dass ein Markt für föderierte Identitätsmanagementsysteme vorhanden zu sein scheint. Entgegen anderen Stimmen in der Literatur und Hoffnungen unter Datenschützern spielt der Privatsphärenschutz aber nur eine geringe Rolle für die Zahlungsbereitschaft.

Digitale Identität nach Snowden
Grundordnungen zwischen deklarativer und relationaler Identität

Christoph Engemann

Die Veröffentlichungen geheimer Dokumente der angelsächsischen Geheimdienste durch Edward Snowden markieren für die Erforschung und gesellschaftliche Diskussion digitaler Identität eine Zäsur. Schon auf Grundlage der derzeit etwa 6.000 Seiten der einsehbaren Dokumente aus Snowdens insgesamt wohl mindestens 250.000 Seiten umfassenden Pakets (ACLU 2015; Cryptome 2015) zeigt sich, dass es in den letzten zwei Dekaden zwei parallel laufende Entwicklungen staatlicher Auseinandersetzungen mit dem Problem digitaler Identität gab. Zeitgleich zu den seit Mitte der neunziger Jahre des vergangenen Jahrhunderts öffentlich und zum Teil erbittert geführten Debatten um die Gestaltung der rechtlichen, technischen und normativen Herausforderungen, Menschen im Internet identifizierbar zu machen, ist innerhalb der Geheimdienste aktiv an Verfahren für die digitale Identifikation von Menschen zu Sicherheitszwecken gearbeitet worden. In ihren Voraussetzungen und Zielen sind diese beiden Entwicklungen fundamental unterschiedlich, jedoch sind sie beide vor dem selben Problemhorizont zu verorten: der Erschütterung des historisch erwachsenen staatlichen Authentifikationsmonopols durch das Internet.

Im Folgenden soll dieses Authentifikationsmonopol in seiner historischen Genealogie skizziert werden um dann zu zeigen, welche Herausforderungen das Internet für diese genuin staatliche Funktion bedeutet. Im Anschluss werden die Techniken und rechtlichen Rahmenbedingungen staatlich und im Rahmen des Rechts zugestellter digitaler Identitäten kursorisch dargestellt. Der Text schließt mit Fragen für die weitere Debatte digitaler Identität und staatlicher Internetpolitik vor dem Hintergrund der mit den Snowden Papieren offenkundig gewordenen Fähigkeiten der Geheimdienste.

1 Staatliche Authentifikationsmonopole: Europa, Amerika und die Geschichte moderner Identitäts-Systeme

Die Fähigkeit Menschen zu identifizieren ist zugleich eine der fundamentalen Leistungen wie auch Funktionsvoraussetzung neuzeitlicher Staatlichkeit. Auf einer basalen Ebene erlaubt sie die Unterscheidung zwischen Bürger und Nicht-Bürger (Opitz 2012: 144 ff.) und damit die Organisation der Ein- und Ausschlussformationen der Bevölkerung eines bestimmten Staates. Auf der individuellen Ebene ist die Unterscheidung Bürger/Nichtbürger folgenreich: Für einen Staatsbürger gelten in wichtigen Bereichen der demokratischen Teilhabe, der Freizügigkeit und des Sozialrechts andere Rechte und andere Pflichten als für eine Person mit Papieren eines anderen Staates – einem Ausländer. Weiterhin ist Identifikation im Sinne der Zuordnung von Handlungen zu Individuen Voraussetzung für die Rechtsprechung und Rechtsdurchsetzung und in liberalen Demokratien darüber hinaus Grundlage für deren Gerechtigkeitsnarrative. Denn der Ausschluss unzuverlässiger oder gar willkürlicher Zuordnungen von Handlungen zu Individuen ist Grundlage für das Vertrauen darin, dass das staatliche Gewaltmonopol nur in legitimer Weise ausgeübt wird. Schon eine Exekutive oder Judikative, die sich diesbezüglich wiederholt erratisch oder inkompetent zeigt, würde in ihrem Status als Garant von Freiheit und Gleichheit schnell in Zweifel geraten. Repräsentanten der Staatlichkeit, die willkürlich Ereignisse und Handlungen Individuen zuschreiben, würden diesen als autokratisch und rechtlos erscheinen lassen. Neben dieser staatlichen Legitimationsdimension sind Identifikationsverfahren aber auch tief in das ökonomische Handeln eingelassen: Das mit dem ökonomischen Austausch einhergehende Statut des Vertrages benötigt das wechselseitige Vertrauen auf die Identifizierbarkeit des jeweils anderen im Konfliktfall für die Durchsetzung der Vertragsbedingungen durch die Staatlichkeit.

Entsprechend wichtig sind die administrativen Verfahren, die es erlauben, innerhalb und an den Grenzen eines Territoriums Menschen mit Identitäten auszustatten und diesen wiederum Handlungen zu attribuieren. Das Ergebnis dieser Operationen, zu denen Personennamen und Identitätspapiere, aber auch Post- und Fernmeldeadressen zu zählen sind, ist die Person als vom Recht adressierbare Instanz. In diesen Kontext gehört auch die unter dem Begriff der Forensik versammelten Verfahren der Beweisermittlung und -sicherung. Diese können dann zur Anwendung kommen, wenn die Attribution von Handlung zu Personen Schwierigkeiten macht und mittels Beweisen rekonstruiert werden soll. Die Einführung und Sta-

bilisierung von Personennamen und Identitätspapieren ist historisch eng mit dem Aufstieg des westfälischen Nationalstaats einerseits, dem Phänomen der Kolonisierung andererseits verbunden und weist eine lange krisenhaften Geschichte auf (Torpey 1998, 2000; Caplan und Torpey 2001; Groebner 2004; Hornung 2005; Siegert 2006; Engemann 2011, 2012b). Die heute für industrielle Gesellschaften so selbstverständliche Tatsache, dass Menschen Vor- und Nachnamen haben, und diese Namen ein Leben lang stabil bleiben, dass diese Menschen zudem postalische Zustellungsadressen haben und über Papiere verfügen, ist historisch verhältnismäßig jung. Die auf diesen Zustand hinführenden Prozesse setzen mit dem Ausgang des Mittelalters Ende des 15. Jahrhunderts ein. Hier sind vor allem die nach der Entdeckung Amerikas beginnenden Kolonisierungen sowie die gleichzeitig stattfindende Reformation und schließlich der Dreißigjährige Krieg anzuführen. Dessen Ende mit dem Westfälischen Frieden von 1648 wird gemeinhin als Gründungsmoment moderner Staatlichkeit markiert. Wie im weiteren zu skizzieren sein wird, dauert es jedoch noch fast 200 Jahre, bis die hier entstehenden staatlichen Formationen die oben genannten Kapazitäten der Adressierung von Menschen ausgebildet haben.

Die Ausgangslage im Mittelalter war grundsätzlich verschieden von der Situation, die modernen Menschen als selbstverständlich erscheint. In den deutschsprachigen Gebieten war bis in das 12. Jahrhundert Einnamigkeit ebenso verbreitet wie die auf römisches Rechtsgut zurückgehende freie Namenswahl (Caplan 2001: 55 & 59; Seutter 1996: 19). Die Historikerin Jane Caplan hält fest: „These relatively fluid naming regimes reflected a system of distinction rather than identification." (Caplan 2001: 55). Für die soziale Distinktion waren vor allem Kleidung, Wappen, bzw. sogenannte „Zaichen" (Groebner 2004: 34) genannte wappenartige Marken, die sichtbar angebracht getragen wurden, von Bedeutung. Ebenso wichtig waren körperliche Narben, die sowohl positive wie negative Stigmata sein konnten. So zeigten bestimmte Narben die Mitgliedschaft in Ordensgemeinschaften ebenso wie die Teilnahme an Pilger- oder Kreuzfahrten an. Andere Narben, wie die sprichwörtlichen Schlitzohren, waren zugleich Strafe wie soziales Signalsystem, das die (fehlende) Vertrauenswürdigkeit einer Person anzeigen sollte (Groebner 2004: 75 f.). Für die gemeine Bevölkerung spielten Personennamen und familiäre Genealogien eine geringe Rolle, und ebenso wenig waren Urkunden mit Angaben über die Namen, die Herkunft und Zugehörigkeit der Person von Bedeutung. Anders beim Adel und Klerus, deren Status, Besitz- und Machtansprüche sich aus ihren familiären Herkünften ableiteten. Bei der Markierung solcher Zuge-

hörigkeiten waren Familiennamen von zentraler Bedeutung und wurden über Urkunden und Siegel bezeugt. Dazu gehörte es auch, bei der Geburt registriert zu werden und über entsprechende Urkunden zu verfügen.

Um die Mitte des 16. Jahrhunderts entwickelten mindestens zwei große administrative Apparate ein Interesse an der Identifikation von Individuen im Sinne ihrer über Zeit und Distanzen hinweg zuverlässigen Wiedererkennung. Es handelt sich zum einem um die katholische Kirche, zum anderen um die spanische Krone. Die großen Schismen des Christentums – in England spaltet sich 1534 unter Henry VIII die anglikanische Kirche von Rom ab, während in Zentraleuropa spätestens mit der Augsburger Konfession von 1530 die Eigenständigkeit des Protestantismus faktisch vollzogen war – zeitigten für die katholische Kirche die Notwendigkeit von Reformen. Auf dem Konzil von Trient hatte die katholische Kirche zwischen 1545 und 1563 nach theologischen und administrativen Antworten auf die Herausforderung des Protestantismus gesucht. Bestandteil der 1563 ergangenen Resolutionen des Konzils war die Verpflichtung der Pfarrer auf das Führen von Kirchenbüchern, in denen die Vergabe aller Sakramente verzeichnet werden sollte. Damit sollte insbesondere jede Taufe und mithin Vergabe eines Namens an einen neugeborenen Menschen auch ein Schriftakt werden. Die Forderungen des Konzils sahen vor, dass das christliche Ritual der Benetzung des Kindes mit Weihwasser fest mit der Niederschrift und Beurkundung dieses Ereignisses zu verknüpfen war. Die Taufe umfasste damit 1. einen Schriftakt, der sowohl dem Individuum einen persönlichen Vornamen und einen Familiennamen zuschrieb, als auch 2. im selben Vollzug die Zugehörigkeit zur katholischen Kirche registrierte. Schließlich war 3. der Empfang eines christlichen Namens mit der Taufe die Herstellung einer Adresse, mit der sich ein Individuum selbst adressieren, und über die seine sozialen, vor allem seine religiösen Beziehungen und Ansprüche organisiert werden konnten. Nur wer getauft ist, kann die weiteren Sakramente über den Lebenslauf in Anspruch nehmen.

Der Personenname bedeutet hier also zugleich Individualität und Zugehörigkeit zu einem Kollektiv. Er ist zudem Effekt eines Medienensembles, das die Verfügbarkeit von stabilen Speicher- und Archivsystemen, die Standardisierung der Niederschrift, sowie Transmissionssysteme zur Übertragung dieser Daten voraussetzt. Dies ist eine Konstellation, die in der Geschichte der Identifikationssysteme ab dem 16. Jahrhundert wiederkehren wird: Der Personenname ist ein medial vermitteltes und stabilisiertes Datum, das zugleich individuell wie sozial figuriert.

Die mit den Beschlüssen des Konzils von Trient geforderte Durchsetzung einer allgemeinen und kontinuierlichen Geburtenregistratur sollte jedoch auch der katholischen Kirche als größtem „entwickelten Bürokratismus“ (Weber 2002: 556) der damaligen Welt nicht gelingen. In vielen Pfarreien wurden keine Kirchenbücher geführt und wo diese vorhanden waren, enthielten sie häufig keine Angaben zum Geburtsdatum und -ort; überdies fehlten häufig auch die Namen der Eltern:

> „Ecclestial registration of this kind was not an unqualified success in any State; entries were occasionally meager and irregularly made; there was an absence of uniformity in the compilation of such records, so that registries relating to different parts of the same country were not of equal value; the system did not apply to the whole of the population…” (Noriel 2001: 27).

Eine solche Aufgabe einer totalen und kontinuierlichen Registratur aller Menschen eines bestimmten Gebietes hatte sich etwa zur gleichen Zeit die spanische Monarchie gestellt. Diese sah sich weniger mit religiösen Spaltungsdynamiken konfrontiert, als mit der Notwendigkeit, auf einem historisch neuen Niveau die administrative Herausforderung des Regierens auf Distanz zu meistern. Der mittelalterliche Herrschaftsmodus des Präsenzkönigtums basierte auf der erlebbaren und wiederkehrenden Präsenz des Regenten in seinem Reich (Kantorowicz 1957; Siegert 2003: 67; Weber 2002: 605). Der Herrscher bereiste fortwährend sein Land und machte sich seinen Untertanen präsent, die seiner Herrlichkeit in komplexen und strukturierten Zeremonien zu huldigen hatten. Die Karlsauen Karls des Großen können hier als paradigmatisches Beispiel gelten. Mit der Entdeckung Amerikas durch Christoph Kolumbus 1492 schrieben sich das spanische Herrscherpaar Felix und Isabelle Gebiete zu, deren persönlicher Besuch aufgrund der Gefahren und Dauer der Atlantikquerungen unrealistisch blieb. An Stelle der Visitationen entwickelte die spanische Administration mithilfe der katholischen Inquisition ein papierenes Substitut der Präsenz der Herrscher auf der anderen Seite des Atlantiks. Mittels eines möglichst lückenlosen und kontinuierlichen Systems der Dokumentation und Registratur, sowie einer fortwährenden Zirkulation der Akten zwischen Spanien und „las indias“ wie die neue Welt genannt wurde, suchte die spanische Krone zugleich am entfernten Ort präsent zu sein, wie diesen an ihrem Ort präsent zu haben. Dies war ein Prozess, dessen Schwierigkeiten und fortwährendes Scheitern über das gesamte 16. Jahrhundert hinweg am spanischen Hof immer neue Innovationen hervortrieb und medienhistorisch als einer der Herkünfte „des Betriebssystems moderner Staatlichkeit“ verstanden werden kann. Besonders Phillip II (1527-1598), von seinen Zeitgenos-

sen „el rey papelero“ genannt, da er sich unermüdlich dem Studium der Akten widmete und beständig ebensolche produzierte (Müller 2012: 58; Siegert 2003: 66) forcierte eine nie gekannte Systematisierung bürokratischen Schreibens. Nicht weniger als eine „entera noticia de la cosas“, also eine vollständige Beschreibung aller Menschen und Dinge der Welt wird 1571 per Erlass gefordert (Siegert 2003: 86). Alle dort lebenden Untertanen waren aufgefordert, sich an der stetigen und möglichst dichten Registratur der Dinge und Ereignisse der neuen Welt zu beteiligen. Was sich ereignete, so die zugrunde liegende Idee, sollte zugleich dokumentiert und so dem im fernen Spanien residierenden König präsent gemacht werden.

Voraussetzung einer solchen niemals endenden und freilich auch unmöglichen Schreibarbeit diesseits wie jenseits des Atlantiks ist das Papier. Papier war ein relativ neuer Schreibgrund, der im Vergleich zum Mittelalter einen entscheidenden Wandel mit sich gebracht hatte. Papyrus, welches im Mittelalter etwa bis an das Ende des 13. Jahrhunderts das vorherrschende Speichermedium (Müller 2012: 44 ff.) gewesen ist, war ein teurer Schreibgrund, der sich einem verschwenderischem Gebrauch, wie in einem modernen Büro erforderlich, verbot (Müller 2012: 61). Papier dagegen war günstig und ermöglichte es, die geforderte umfassende und unendliche Aufzeichnung aller Dinge zur Durchführung zu bringen. Zugleich hatte ein solcher bürokratischer Furor eine Standardisierung und Normierung der Abläufe und Formate erfordert (Siegert 2003: 89 f.; Vismann 2000: 154 f.). Schließlich (und das ist für den hiesigen Argumentationsgang zentral) zeitigte sie aber auch eine weitere Entwicklung, nämlich die Dokumentation und Registratur von Menschen, die nach den „las indias“ reisen wollten, bzw. von dort kamen. Wie gesagt umfasste die „entera noticia de la cosas“ gerade nicht nur die Dinge und die Ereignisse, sondern auch die Menschen. Deren Adressierbarkeit setzt die Dokumentation und Registratur ihrer Namen voraus. Wie oben angeführt war dieses aber bislang ein Privileg, das bislang dem Adel und dem Klerus vorbehalten gewesen war. Mit der Kolonisierung Amerikas wird dieses Privileg des Aufgeschrieben-Sein jedoch aus seinen ständischen Kontext gelöst und auf den gemeinen Menschen angewandt. Im selben Jahrhundert also, indem die katholische Kirche die Einführung der Geburtenregistratur verfügt und in Europa durchzusetzen versucht, unternimmt die spanische Krone, selbst katholisch und von der Inquisition unterstützt, den Versuch, eine ganze Population zu registrieren – in diesem Fall die Population der Passagiere, also derjenigen Menschen, die zwischen Spanien und Amerika zirkulieren.

Der spanische Fall bleibt eine Ausnahme und zwischen dem 16. und 18. Jahrhundert sind innerhalb Europas die Veränderungsprozesse, die den modernen Personenstatus mit hervor bringen, eher graduell Natur. Dazu zählt insbesondere im 17. Jahrhundert das Postwesen, das Menschen unterschiedslos, also unabhängig von der Zugehörigkeit zu Adel und Klerus, adressierbar machte (Siegert 1993). Damit zusammenhängend, aber wesentlich durch das Begehren nach der Konskription wehrfähiger Männer motiviert, war die Einführung von Hausnummern (Tantner 2007). Vor allem aber beginnen die absolutistischen Staaten im Laufe 18. Jahrhundert, in ihren Bevölkerungen die Geburtenregistratur einzuführen. Die nach der Reformation von der katholischen Kirche als Mittel zur Kontrolle ihrer Population eingeführte Methode erfährt eine sukzessive Säkularisierung und ist gegen Ende des 18. Jahrhunderts in einigen europäischen Ländern als staatlich organisierter Prozess üblich (Noriel 2001).

Die Französische Revolution markiert sodann mit ihrer eruptiven Beseitigung der absolutistischen Herrschafts- und Verwaltungsstrukturen das wichtigste Datum auch in der Geschichte moderner Identifikationsadministration und der Monopolisierung der Authentifikation von Menschen durch die Staatlichkeit. Im Zuge der Revolution wird die allgemeine und unterschiedslose Geburtenregistratur und Standardisierung des Namenssystems hin zu einem patrilinearen Vornamen-Nachnamen System eingeführt (Caplan 2001; Noriel 2001). Sie gelten als die administrative Grundlage des Bürgerstatus und Garanten von Freiheit und Gleichheit. Teil dieser Entwicklung sind Erlasse zur Unveränderbarkeit des Namens über den Lebenslaufs, die die Verwaltung des Zivilstatus der Bürger erlauben soll (Noriel 2001). Dazu zählen zunächst Unterscheidungen wie verheiratet/nicht-verheiratet, aber auch Kriminalitätsregister sowie der Konskriptionsstatus und basale Sozialleistungen. Die französischen Entwicklungen bleiben im weiterhin monarchistischen Rest Europas keineswegs eine Anomalie. Im Gegenteil kommt es in der ersten Hälfte des 19. Jahrhunderts mit Ausnahme von England in fast allen nordeuropäischen Staaten zur Übernahme der im Zuge der Französischen Revolution eingeführte Verfahren der Geburtenregistratur und Verrechtlichung der Namensvergabe (Caplan 2001; Noriel 2001; Torpey 1998). Die Namensvergabe wurde nun ein Akt unter staatlicher Begleitung: Der von den Eltern gewählte Taufname fand Eintrag in eine staatliche Geburtsurkunde, und der Akt der Benamung war damit zugleich der Akt der Registratur eines Bürgers. Der so aufgezeichnete Name sollte als die Adresse fungieren, unter der der Bürger forthin bei allen Verwaltungsakten anzusprechen war. Im Deutschen Reich kommt

es mit der Bismarck'schen Sozialgesetzgebung in den 1870er Jahren und schließlich zur Wende zum 20. Jahrhundert mit der Einführung des Bürgerlichen Gesetzbuchs (BGB) zu einer endgültigen Verfestigung der Rechtsnormen bezüglich Geburtenregistratur und Namensrecht (Seutter 1996).

Parallel zu diesen hier kursorisch und gerafft wiedergegeben Entwicklungen, sind zwei weitere Schauplätze für die Entwicklung der modernen Identitätsverwaltung wichtig: zum einen der in der zweiten Hälfte des 19. Jahrhunderts sich institutionalisierende Diskurs der Kriminalistik mit ihrer wichtigen Teildisziplin, der Forensik, zum anderen der Kolonialismus, der wie oben gezeigt bis auf das 16. Jahrhunderts zurück geht. In beiden Kontexten wird der Körper als Identifikationsressource verhandelt, und sie stellen Vorläufer der heutigen Biometrie dar. Historisch gehören sie zum Wandel weg vom „writing on the body" (Caplan und Torpey 2001) in der Zeit nach etwa 1820. Gemeint ist die nicht erst seit dem Mittelalter gängige Praxis, den Körper gleichsam als Schreibgrund zu benutzen, um so einen sozialen Staus auszuweisen. Bekannt sind hierbei vor allem die negativen Varianten der Markierung von Kriminellen oder aus anderen Gründen Ausgestoßenen, wie Kranken, Häretikern oder Sklaven. Es gab aber auch sozial valuierte Formen, vor allem in religiösen Kontexten, wo bestimmte Tätowierungen als Ausweise von Pilgerfahrten galten. In beiden Fällen wurde die menschliche Haut „als Dokument, Urkunde, Archiv" (Groebner 2004: 70) genutzt. Im Laufe des 19. Jahrhunderts treten an die Stelle des in-den-Körper-Schreibens Verfahren des „reading the body" (Caplan und Torpey 2001: 8). Der Körper wird nicht mehr als Schreibgrund behandelt, sondern figuriert gleichsam als je individuell auszulesende Ressource für das Identifikationsbegehren der Staatlichkeit (Wichum 2016). In der gesamten zweite Hälfte des 19. Jahrhunderts und teilweise darüber hinaus werden in verschiedenen wissenschaftlichen und bürokratischen Kontexten Methoden gesucht, die es erlauben sollen, Körper vermessbar und dokumentierbar und zu machen.

Es ist jedoch nicht das Problem der Kriminalität, von dem diese Entwicklungen ihren Ausgang nehmen. Hintergrund ist vielmehr, dass die Menschen in den Kolonien in den Augen der offiziellen Machthaber „looked bewilderlingly homogenous," (Cole 2001). Koloniale Subjekte erschienen den europäischen Betrachtern also ununterscheidbar gleich. Es darf angenommen werden, dass auch die jeweils benutzten Namen für die Kolonisatoren unverständlich und schwer memorierbar blieben, und zudem die Alphabetisierung der kolonisierten Bevölkerungen auf wenige

Gruppen beschränkt blieb. Wo weder Augenschein noch Namen als Identifikationsmittel herhalten konnten und die noch junge Photographie zu aufwendig war, waren andere Methoden gefragt, um den Körper als Identifikationsressource zu nutzen. Insbesondere britische Kolonialbeamte begannen ab Mitte des 19. Jahrhunderts für Verträge und Formulare Fingerabdrücke abzunehmen.

Neben der Durchsetzung der britischen Rechtsprechung, insbesondere nach Aufständen und Meutereien (Beavan 2001: 42; Cole 2001: 64), war der Missbrauch bei Pensionszahlungen ein wesentliches Problem:

> „British officials responsible for disbursing pensions could not tell one Indian from another." (Cole 2001: 64)

Es ist die Adressierung sozialstaatlicher Allokationen, die durch die offenbar gängige Praxis, sich die Identität eines verstorbenen Empfängers von britischen Pensionszahlungen anzueignen, problematisch wird. Pensionsansprüche konnten im Rahmen von Militärdiensten oder durch die Arbeit in der Kolonialverwaltung erworben werden. Ob jedoch eine Person diejenige war, für die sie sich ausgab, oder ob dieser Körper, der sich als Anspruchsberechtigter präsentierte, ein anderes Individuum mit einem anderem Namen war, ließ sich in den kolonialen Kontexten offenbar nicht allein anhand der entsprechenden Namen und Papiere feststellen.

Die Geschichte der im 20. und 21. Jahrhundert so umstrittenen Sozialstaatlichkeit kennt also auch koloniale Schauplätze, an denen sich Körper unter falschen Namen zur Adresse von Wohlfahrtsinterventionen machten, welche gar nicht ihnen gelten sollten. Der britische Kolonialbeamte William Herschel, der ab 1858 als erster nachweisbar mit Finger- und Handabdrücken zur Überprüfung der Anspruchsberechtigungen indischer Pensionsbezieher experimentierte, hielt fest, dass dieses Problem nicht allein für Indien Gültigkeit hatte: „first I used it for pensioners whose vitality has been a distracting problem to governments in all countries" (Cole 2001: 64). In diesem Kontext und über eine Reihe weiterer Stationen entstehen die Verfahren der Daktyloskopie, also der Identifikation mittels der Abnahme und Klassifizierung von Fingerabdrücken. Die wesentliche Innovation der Daktyloskopie bestand nicht im bloßen Abnehmen von Fingerabdrücken, sondern in der Übersetzung des Abdrucks in alphanumerische Zeichenfolgen, die in Karteikarten aufschreibbar und übertragbar waren. Die verschiedenen Verfahren beruhen dabei auf dem Auszählen der wirbel- und schleifenförmigen Muster an den Fingern, die in einem zweiten Schritt mit Zahlen- und Buchstabenwerten versehen wurden. Aus den

Fingerabdrücken einer Hand konnte somit eine Buchstabenfolge wie z.B. WL.-LW-LW-LL-Wl werden, die nicht nur die Einordnung einer entsprechenden Karteikarte in einem Register erlaubte, sondern auch die Versendung dieser Daten und damit die Identifikation derselben Person an verschiedenen Orten.

In Europa dagegen ist die noch junge Forensik ab etwa 1880 zunächst von dem Anthropometrie genannten System des französischen Polizeibeamten Francois Bertillon dominiert. Bertillons System suchte Menschen über die Vermessung von elf Körperteilen eindeutig zu identifizieren (Cole 2001: 76; Wichum 2016). Die Wiedererkennungsleistung beruhte dabei genau wie bei den daktyloskopischen Verfahren auf einer cleveren Übersetzung der Messergebnisse in alphanumerische Codes, welche die schnelle Sortierung großer Mengen von Karteikarten erlaubten. Körpervermessung und Karteikarten ergaben hier ein System, indem ein einmal aufgezeichnetes Individuum anhand des Kürzelsystems zur Repräsentation von Körpermerkmalen wiederauffindbar war. Vor allem aber waren diese Kürzel als Folge diskreter Symbole telegraphisch übertragbar. Mithin erlaubte die Bertillonage auf der Grundlage einer einmaligen Aufzeichnung „identification at a distance" (Cole 2001: 217). Ein Mensch konnte an einem beliebigen Ort einer anthropometrischen oder daktyloskopischen Messung unterzogen, die Daten per Telegraph oder Post übertragen und die Person auf Grundlage einer Registerabfrage identifiziert werden. Menschliche Körper waren nicht nur aufschreibar und speicherbar sondern metaphorisch gesprochen auch übertragbar geworden: „Bertillion reduced the body to language and then to code – turning the criminal body into pure information (Cole 2001: 49)."

Um das Jahr 1900 ist somit eine Situation zu verzeichnen, in der einerseits die aus kolonialen und kriminologischen Kontexten stammenden Verfahren der Biometrie, andererseits die Konsolidierung des Namensrechts und der Geburtenregistratur in Verbindung mit frühen Formen der Sozialstaatlichkeit zur Folge haben, dass staatlicherseits Menschen als identifizierbare und damit unterscheidbare Personen gelten. Für die Gouvernemedialität – also die Formen der Problematisierung und Regierbarmachung der Medien des Regierens – (Engemann 2011; Engemann und Traue 2006; Sieber 2014) sind diese Verfahren von zentraler Bedeutung. Die Geschichte moderner Staatlichkeit ist durch die Zueignung des Anspruchs charakterisiert, exklusiv bestimmte Medienensembles als identitätsstiftend deklarieren zu können. Entsprechend kann von einem staatli-

chen Authentifikationsmonopol gesprochen werden, das unter den medialen Monopolen der Staatlichkeit eine besondere Position aufweist:

> „Dem Gewaltmonopol des Staates entspricht so gesehen auch ein mediales Monopol – bestimmte Typen von Dokumenten dürfen nur von den zuständigen Stellen verfertigt werden, Fälschungen werden schwer bestraft (nach § 267 des StGB mit Geldstrafen oder Haftstrafen bis zu fünf Jahren)." (Schröter 2015: 13)

Weder dürfen Menschen sich selbst Identitäten und entsprechende Papiere ausstellen, noch steht es wirtschaftlichen oder religiösen Institutionen frei, mit dem Staat bei der Vergabe solcher Identitätsdokumente zu konkurrieren. Kern dieses medialen Monopols sind die Register, denn erst der Eintrag eines Dokuments stiftet dessen Gültigkeit. Im Falle von Identitätsdokumenten ist das unmittelbar anschaulich:

> „Eine Person ist gleich ein Ausweis plus ein interner behördlicher Ausweis über den ausgestellten Ausweis, also eine Kanzleikopie oder ein Registereintrag." (Groebner 2004: 168)

Einzig in den einschlägigen staatlichen Registern verzeichnete Dokumente werden als Authentifikationsmedien akzeptiert, und es ist die Staatlichkeit, die deren Verwaltung organisiert. Monopolisierung bedeutet dabei nicht notwendig die Zentralisierung dieser Register, wohl aber die Vereinheitlichung ihrer Anlage sowie der Datenformate und Protokolle, mit denen Menschen Papiere erhalten. Solche Papiere erlauben nicht zuletzt die „identification at a distance", da unabhängig vom Aufenthaltsort die darauf befindlichen Daten auf ihre Konsistenz mit den staatlicherseits vorgehaltenen Registereinträgen überprüft werden können. Der Soziologe John Torpey stellt diese Entwicklung in den Kontext dessen, was er die „monopolization of the legitimate means of movement" nennt (Torpey 1998):

> „they [die Staatlichkeit C.E.] have monopolized the authority to restrict movement vis-a-vis other potential claimants, such as private economic or religious entities. Such entities may play a role in the control of movement, but they do so today at the behest of states."

Nicht die Kontrolle der Bewegung von Menschen – und hinzuzufügen die Kontrolle von Dingen – suchen Staaten zu erlangen, sondern sie monopolisieren das Recht, die Bewegungsfreiheit unter bestimmten Bedingungen einzuschränken. Innerhalb eines gegebenen Territoriums hat sich die Staatlichkeit das Monopol und die Mittel zur Durchsetzung dieses Rechts angeeignet. Zu diesen Mitteln gehören die gesetzlichen Bestimmungen, die festlegen unter welchen Bedingungen Menschen oder Güter kontrol-

liert, festgesetzt oder im Falle von Gütern beschlagnahmt werden dürfen. Dazu zählen weiterhin die Einrichtung der Exekutivgewalten wie der Polizei, der Zollbehörden, aber auch der Finanzbehörden mit ihren Kompetenzen, Transaktionen zu kontrollieren und zu unterbinden. In allen Fällen ist die Voraussetzung für eine solche Interventionsfähigkeit in die Bewegungsfreiheit die Verfügbarkeit zuverlässiger Mittel zur Identifizierung von Menschen. Entsprechend unterhält jeder moderne Nationalstaat Verfahren zur Authentifikation und Registratur und damit zur Identitätsfeststellung seiner Bürger. Dabei geht es nicht um eine Kontrolle aller Bewegungen, sondern wie gesagt darum, diese unter bestimmten und rechtlich geregelten Bedingungen einschränken zu können. Torpey betont diesbezüglich ausdrücklich:

> „...I am not claiming that states and the state system effectively control all movements of persons (...)" (Torpey 1998).

Vielmehr ist es im Gegenteil ein Spezifikum moderner Staatlichkeit, einerseits die individuelle Bewegungsfreiheit zu eskalieren und andererseits die Kontrolle derselben auf bestimmte Situationen und spezifische Orte zu beschränken. Letztere sind die Grenzen des Territoriums, besonders geschützte Gebiete oder Anlagen, ersteres Ereignisse wie Demonstrationen und besondere Sicherheitslagen bis hin zum Ausnahmezustand. Hier sind die Schwellen sowohl für die Kontrolle der Personalien als auch für die Einschränkung der Bewegungsfreiheit herabgesenkt. Innerhalb eines Hoheitsgebiets gilt, dass die Verfahren der Ermöglichung von Bewegungsfreiheit und der Bewegungsversagung an die Identifizierbarkeit der fraglichen Instanzen – ob Menschen oder Dinge – gebunden sind. Die zugrundeliegenden logischen und zeitlichen Sachverhalte sind komplex: Die Freizügigkeit ist ein hohes Rechtsgut, dass wie oben gesagt nur unter besonderen Bedingungen Einschränkung erfahren darf. Zugleich ist, wie zu Beginn dieses Texts dargelegt, jedes Recht auf die Adressierbarkeit von Individuen angewiesen. Alle Menschen genießen innerhalb eines gegebenen Territoriums Freizügigkeit, solange bis sich herausstellt, dass sie nicht identifiziert werden können. Der Kontrollfall ist in liberalen Demokratien eine Einschränkung in die Bewegungsfreiheit, der Ausnahme sein soll, aber vom Regelfall ausgeht, dass Menschen Namen und Papiere haben und damit im Kontrollfall nachweisen können, über gültige Dokumente zu verfügen. Dazu gehören Ausweise, Pässe, Aufenthaltstitel oder auch Geburtsurkunden. Können die Betroffenen von den dazu befugten staatlichen Stellen nicht mit Hilfe solcher Dokumente identifiziert werden, so behal-

ten sich Staaten vor, diese Menschen erkennungsdienstlichen Verfahren zu unterwerfen, sie in ihrer Bewegungsfreiheit einzuschränken oder sie sogar aus dem Staatsgebiet zu entfernen.

Auch bei der Einschränkung der Zirkulation von Gütern kommen Identifikationsmechanismen zum Zuge. Zwar unterliegen diese mit Ausnahme bestimmter pharmakologischer oder gefährlicher Stoffe keiner staatlich geforderten Registratur, jedoch sind die Verfahren, mit denen beispielsweise der Zoll die Herkunft und Beschaffenheit eines Produkts zu prüfen berechtigt ist, genau geregelt. Hier ist die Bewegungsversagung Registratur: der Moment, in dem sich die staatlichen Stellen in die Zirkulation einschalten, ist ein Akt der bürokratischen Dokumentation und Identifikation des fraglichen Gutes und häufig auch seiner Eigentümer und Besitzer.

Die zugrunde liegende Interessenlage ist dabei paradox: Eine florierende Wirtschaft profitiert von der Freizügigkeit der Bürger und der ungehinderten Zirkulation der Güter. Zugleich gilt eben diese Freizügigkeit und ungehinderte Zirkulation als potentiell destabilisierend. Entsprechend müssen Nationalstaaten Bewegungsfreiheit zugleich sowohl einschränken als auch befördern (Salter 2003: 58). Beispiele für solche Bewegungseinschränkungen sind das Strafprozessrecht, das die Festsetzung von Verdächtigen und Straftätern erlaubt, oder das Ausländerrecht, das die Bewegungsfreiheit der betroffenen Individuen einschränkt. Auf der Ebene der Dinge sehen beispielsweise das Zollrecht und das Gefahrgüterrecht Regelungen zur Einschränkung ihrer Zirkulation im Staatsgebiet vor.

Salters Argumentation läuft also darauf hinaus, dass legitime Nutzer eines Rechts wie der Bewegungsfreiheit nur diejenigen sind, die einer vorangegangene Registratur unterzogen wurden. Diese kann zeitlich sehr lang zurück liegen und beispielsweise im Zusammenhang mit der Geburt erfolgt sein, deren Registratur zugleich den Zugang zum Staatsbürgerstatus mitbestimmt. Sobald man sich innerhalb eines Staatsgebietes und besonders dann wenn man sich über seine Grenzen hinweg bewegt, kann dieses Privileg der Bewegungsfreiheit im Kontrollfall beim Fehlen entsprechender Papiere entzogen werden. Akzeptiert werden nur solche Papiere, die entweder im eigenen staatlichen Register verzeichnet sind, oder die von einem anerkannten Drittstaat stammen. Kann die Person den Besitz solcher Dokumente nicht nachweisen, so haben staatliche Stellen die Autorität, sie an der Weiterreise zu hindern.

Die Entwicklung und allgemeine Anwendung von Identifikationsmedien sind somit Teil der von Salter beschriebenen „monopolization of the legitimate means of movement." Wie ausgeführt, sind sie zudem Vorausset-

zung sowohl des ökonomischen Verkehrs als auch der Sozialstaatlichkeit und nicht zuletzt der Organisation der Trennung der eigenen Bevölkerung von anderen Gruppen. Seit dem Entstehen der neuzeitlichen Staatlichkeit in der Mitte des 17. Jahrhunderts sind papierbasierte Verfahren deren mediale Grundlage gewesen. Staatliche Bürokratien waren Papiermaschinen und sind es trotz des Internets bis heute weitgehend immer noch (Vismann 2000; Siegert und Vogl 2003; Chamayou 2012; Hull 2012; Kittler 2012; Müller 2012; Buschmann 2014). Insbesondere diejenigen Funktionen, die das hier umrissene Authentifikationsmonopol ermöglichen, basieren auf dem Prozessieren von Papier. Der Bürger hatte gleichsam eine papierene Identität, die aus einem ausgeklügelten System von aufeinander verweisenden Papieren bestand. Den individuellen Geburtsurkunden, Pässen und Ausweisen stand jeweils eine Registerkopie derselben in einer staatlichen Stelle gegenüber. Wie tief und zentral diese Medien in den Alltag eingelassen sind, illustrieren die Schwierigkeiten der „sans-papier" (Derrida 2005: 57; Chamayou 2012: 136 f.), also der Menschen, die innerhalb moderner Nationalstaaten ohne solche Dokumente ihr Dasein fristen.

In der Zusammenfassung der bis hier her geschilderten Genealogie neuzeitlicher Identitätszuschreibung wird deutlich, dass in dem historisch gewachsenen und bis zum Aufkommen des Internet geltenden staatlichen Authentifikationsmonopol vier Elemente miteinander in einem komplexen System zusammenwirken: das Papier als Speichermedium, staatlich monopolisierte Register, der Körper als Letztbezug der Adressierung, und das Territorium als räumliches Bezugssystem dieses Identitätskonstrukts. In diesem Regime werden innerhalb eines gegebenen Territoriums Menschen mit nach einheitlichen Formaten gestalteten und in staatlichen Registern verzeichneten Papieren versehen, die es ermöglichen sollen, sie unter bestimmten, gesetzlich genau definierten, Umständen körperlich wiederzufinden, bzw. sie an der Verbringung ihrer Körper zu hindern. Man kann diese Konstellation deklarative Identität nennen, da hier eine bestimmte Instanz – der Staat – die mittels eines definierten Sets medialer Operationen gestifteten Dokumente als Identitäten setzt.

2 Papierloser Raum: das Internet und die Krise des staatlichem Authentifikationsmonopols

Das bis hierher beschriebene Format deklarativer Identität hat sich in einem langen Prozess zwischen der beginnenden Neuzeit im 16. Jahrhun-

dert und der Mitte des 20. Jahrhunderts entwickelt. Etwa mit Ende des zweiten Weltkriegs und dem gleichzeitigen Beginn der Dekolonialisierung ist es idealtypisch in den Industrienationen der ersten Welt implementiert. Zu diesem Zeitpunkt setzen aber bereits Entwicklungen ein, die einen profunden Medienwandel der Staatlichkeit mit sich bringen, der spätestens ab den neunziger Jahren des letzten Jahrhunderts die historisch gewachsenen Verfahren deklarativer Identität in Frage stellt. Es ist der Computer, der im Zuge der Verwaltungsautomation schon in den späten fünfziger Jahren zunächst als unterstützendes Medium bei der Erstellung und Verwaltung deklarativer Identitäten dient, aber spätestens mit seiner Vernetzung und allgemeinen Verbreitung dieses Format der Identitätsstiftung und seine staatliche Monopolisierung in Frage gestellt hat. Sobald im Zuge der Vernetzung aus Computern das Internet geworden ist, entsteht eine neue Situation, in der die staatlichen Verfahren der Identitätsstiftung kritisch werden. Allgemein sichtbar wird dies ab den frühen neunziger Jahren, als das Internet in das öffentliche Bewusstsein tritt und zugleich erste Anläufe unternommen werden, das staatliche Authentifikationsmonopol auch in digitale Netzen zu übersetzen (Engemann 2015). Denn für das Internet sind die beschriebenen papierbasierten Verfahren der Identitätsadministration unbrauchbar, und wie zu zeigen sein wird, bringt dieses Medium Alternativen zum Format der deklarativen Identitäten mit sich. Insbesondere steht das staatliche Authentifikationsmonopol deshalb seit Mitte der neunziger Jahre des 20. Jahrhunderts nachhaltig in Frage. Papiere gelten im Internet nichts und staatliche Instanzen haben Schwierigkeiten, Handlungen im Internet zuverlässig Personen und ihren Körpern zu attribuieren. Wessen Hände an einem Keyboard oder einem Touch-Display waren und beispielsweise eine E-Mail versendet haben, ist der E-Mail-Nachricht anders als auf dem Papier bei einer eigenhändigen Unterschrift nicht eingeschrieben. Insbesondere im gerichtlichen Verfahren ist jedoch eine solche über die Eigenhändigkeit gestiftete Verknüpfung von Dokument und Körper oftmals ein wichtiger Teil der Indizienkette (Hertel et al. 2004: 725). Angesichts der Bedeutung des Internets für das Alltagshandeln und der fortschreitenden Untrennbarkeit von Online- und Offlinewelt, wächst der Anspruch von staatlicher Seite, auch in und mit digitalen Medien Menschen zuverlässig identifizieren zu können. An die Stelle eines Bürgers mit einer papierenen Identität soll ein Bürger mit einer digitalen Identität treten.

Die Regierungen von Staaten wie den USA und verschiedener europäischer Länder sind bereits seit den neunziger Jahren wiederholt mit einer Reihe von Initiativen hervorgetreten, für das Internet ähnlich belastbare

Identifikationsverfahren wie für die reale Welt zu etablieren (Hornung 2005: 93–126; Kubicek und Noack 2010; Engemann 2015). In Deutschland sind hier die qualifizierte elektronische Signatur, der neue Personalausweis, die elektronische Gesundheitskarte und das De-Mail Verfahren zu nennen. Vergleichbare Chipkarten wie der deutsche Personalausweis sind mit unterschiedlichem Erfolg in einigen europäischen Nachbarländern eingeführt worden, und die europäische Union forciert derzeit deren Harmonisierung (siehe Bender in diesem Band, Hornung 2012, 2005). In den USA gab es nach einem umstrittenen Anlauf seitens der Clinton-Administration aus dem Jahr 1994 bis 2011 keine nennenswerten diesbezüglichen öffentlichen Initiativen (Froomkin 1995; Corwin 1998; Covell et al. 1998; Brin 1998; Engemann 2015). Gemeinsam ist sowohl den europäischen als auch den amerikanischen Vorhaben, dass sie an ihren eigenen Ansprüchen gemessen bislang weitgehend gescheitert sind, denn im Alltag der Internetnutzer spielen die hier entwickelten Authentifikationsinstrumente kaum eine Rolle.

Trotz der fundamentalen politischen Unterschiede zwischen Europa und den USA, die insbesondere beim Datenschutz immer wieder zutage treten, gibt es auf der technischen Ebene der neuen Identifikationsverfahren entscheidende Gemeinsamkeiten, die für die weitere Argumentation erläuterungswürdig sind. Grundlage der Authentifikation und Identifikation im Internet sind kryptographische Innovationen aus den siebziger Jahren des 20. Jahrhunderts (Kahn 1996: 982 f.; Singh 1999: 323 f.). Die Grundbegriffe der Public-Key-Kryptographie sind in diesem Band im Beitrag von Lexi Pimenidis wiedergegeben, sollen hier aber noch einmal kurz vergegenwärtigt und am Beispiel des neuen Personalausweises illustriert werden. Seit November 2010 wird dieses neue Dokument in der Bundesrepublik Deutschland ausgegeben und enthält einen kryptographischen Chip, der neben biometrischen und anderen Identitätsdaten über zwei Funktionen verfügt: den elektronischen Identitätsnachweis und die qualifizierte elektronische Signatur. Erstere Funktion wird in diesem Text nicht näher behandelt, sie soll jedoch dem Identitätsnachweis beispielsweise gegenüber Internetanbietern dienen, Die zweite Funktion der qualifizierten elektronischen Signatur erlaubt darüber hinaus in digitalen Umgebungen – online wie offline – digitale Signaturen abzulegen und damit eine rechtlich der eigenhändigen Namensunterschrift weitgehend gleichgestellte Form, Dokumente zu signieren (Hornung 2005: 314). Die begriffliche Unterscheidung zwischen elektronischen und digitalen Signaturen ist dabei nicht zufällig. Digitale Signaturen werden vom Gesetzgeber als Unter-

gruppe von elektronischen Signaturen betrachtet (Langenbach, Ulrich 2002: 10f; Hornung 2005: 70). Der Hintergrund ist hier, dass eine Festlegung auf den Begriff „digital" nicht-digitale Krypto-Verfahren für zukünftige Identitätslösungen ausschließen und dann Gesetzesänderungen notwendig machen würde. Jedoch bieten digitale Signaturen beim gegenwärtigen Stand der Technik das höchste Sicherheitsniveau und sind somit Grundlage der in den meisten Ländern aufgebauten Authentifikationsinfrastruktur. In Deutschland sind der neue Personalausweis und die elektronische Gesundheitskarte mit entsprechenden Chips ausgestattet.

Als Teil einer Public-Key Infrastruktur enthalten die Chips vereinfacht gesagt für die digitale Signatur eine als privater Schlüssel bezeichnete kryptographische Chiffre. Ein mathematisch mit dem privaten Schlüssel verwandter und arithmetisch eindeutig als solcher verifizierbarer öffentlicher Schlüssel wird in einem staatlich anerkannten und über das Internet erreichbaren Trust-Center vorgehalten. Das einschlägige Signaturgesetz bezeichnet solche Trust-Center als Zertifizierungsdiensteanbieter (ZDA). Bei der digitalen Signatur beruht die Funktionslogik darauf, dass der ZDA als ausgebende Stelle die Zugehörigkeit der Schlüssel zu bestimmten Personen mittels eines Zertifikats garantiert. Das Signaturgesetz fordert diesbezüglich, dass der ZDA „die Person (...) zuverlässig zu identifizieren" habe (§ 5 Absatz 1 SigG). Für das Zertifikat gilt außerdem, dass es den Namen des Signaturschlüssel-Inhabers (§ 7 Absatz 1 SigG) oder ein „zugeordnetes, unverwechselbares Pseudonym, das als solches kenntlich sein muss" enthalten muss. Zwischen dem staatlicherseits registrierten Personennamen und dem Zertifikat der digitalen Signatur soll also ein nachweisbarer Zusammenhang bestehen. Faktisch prüft der ZDA anhand eines amtlichen Dokuments wie dem Personalausweis die Identität des Antragsstellers und ordnet ihm auf dieser Grundlage ein für die digitale Signaturfunktion geeignetes elektronisches Zertifikat zu.

Auch bei diesen digitalen Authentifikationsverfahren tritt also wieder das Register als entscheidende Funktionsstelle auf. Digitale Signatur bedeutet digitale Registratur, und eine kritische Frage für die Zukunft des staatlichen Authentifikationsmonopols ist die Kontrolle der Register über die Zuordnung von Person und kryptographischem Schlüssel. Im Vergleich zum historischen Vorbild hat sich mit dem digitalen Wandel eine Verschiebung in der Organisation dieser Zuordnung ergeben. Denn nach deutscher Gesetzeslage ist mit den ZDA ein neuer Intermediär zwischen staatlichen Registern und ihren digitalen Versionen getreten. Im digitalen Raum laufen Abfragen der Gültigkeit eines jeweiligen Zertifikates nicht

über eine staatliche Stelle, sondern werden von den privatwirtschaftlich oder genossenschaftlich betriebenen Trust-Centern der ZDA übernommen. Einschlägige Betreiber solcher Trustcenter sind beispielsweise die Telekom, die Bundesnotarkammer, die von den Sparkassen betriebene S-Trust und die zur Bundesdruckerei gehörende D-Trust GmbH (vgl. die bei der Bundesnetzagentur vorgehaltene Liste unter www.nrca-ds.de).

Dennoch handelt sich bei der digitalen Identität des deutschen Bürgers um eine Verweiskette, in der die staatliche Registratur eine entscheidende Rolle spielt. Seit der ersten einschlägigen Signaturgesetzgebung aus dem Jahre 1999 hat der deutsche Staat bislang darauf bestanden, dass seine bestehenden Register auch für die digitale Identität des Bürgers genutzt werden sollen. Erstens indem wie oben geschildert nach § 5 und § 7 SigG die durch die ZDA ausgestellten Zertifikate auf Grundlage staatlicher Identitätspapiere zugewiesen werden. Zweitens übernehmen im Falle des neuen Personalausweises die örtlichen Meldestellen selbst die realweltliche Authentifikation und Registratur und attribuieren auf dieser Basis der Person ein Schlüsselpaar und damit eine digitale Identität. Die privaten Schlüssel für die digitale Signatur sind im Personalausweis gespeichert, während die zugehörigen öffentlichen Schlüssel über die Trustcenter im Internet abrufbar vorgehalten werden. Im Fall der Prüfung einer mittels eines solchen Zertifikats signierten Transaktion fließen zwischen den Personalausweisen der Kommunikationspartner und den Trustcentern verschlüsselte Daten hin und her, für die mathematische eindeutige Beweise erbracht werden können, welche Chiffrierschlüssel beteiligt waren. Da die im Chiffrierverfahren genutzten privaten Schlüssel auf Grundlage staatlicher Identitätsdokumente von den ZDAs natürlichen Personen zugeordnet wurden, können die so entstehenden Daten als eindeutig auf eine Person verweisend gelten und sind rechtlich auch als solche anerkannt. An die Stelle der sprichwörtlichen Papiere sind hier nach staatlichen Vorgaben registrierte kryptographische Zertifikate und die Chipkartenausweise als ihre Trägermedien getreten.

Es handelt sich bei diesem System um eine digitale Re-Medialisierung des Formats deklarativer Identitäten. Auch hier definiert die Staatlichkeit ein Set medialer Operationen zur Identitätsstiftung, in dem Menschen mit nach einheitlichen Formaten gestalteten und auf staatliche Register verweisenden Bescheinigungen ausgestattet werden. Diese Bescheinigungen – Zertifikate, die im Medienverbund aus neuem Personalausweis und ZDAs erzeugt werden – sollen es ermöglichen, die digitalen Akte eines Individuums einer Person attribuieren zu können. Da diese Regelung des

deutschen Staats nur innerhalb der eigenen Jurisdiktion gelten kann, zudem für ausländische ZDAs besondere Regelungen gelten, bildet auch hier das Territorium das Bezugssystem des Identitätskonstrukts und soll innerhalb dessen die Zuordnung von – digitalen – Handlungen zu Körpern erlauben. Der wesentliche Unterschied liegt in der Form der Speichermedien: An die Stelle von Papier treten Chipkarten und digitale Register in Form von in Trustcentern betriebenen Datenbanken, die die öffentlichen Schlüssel vorhalten.

Im Vergleich zum papierbasierten Format deklarativer Identität handelt es sich bei dieser Entwicklung jedoch nicht um die Etablierung einer Entsprechung des staatlichen Authentifikationsmonopols im Internet. Das ist angesichts der Globalität elektronischer Netzwerke und der einhergehenden Schwierigkeit, analog zum Territorium Unterscheidungen zwischen Innen und Außen treffen zu können, gegenwärtig kaum möglich. Vielmehr liegt beim jetzigen Stand eine Hierarchisierung der Instanzen vor, die im Internet Identitäten vergeben. Innerhalb dieser Hierarchie versuchen Nationalstaaten, sich an die Spitze zu stellen, indem sie beanspruchen, die einzig gültigen Quelldokumente für rechtskonforme digitale Identitäten bereitzustellen. Von Unternehmen, Privatpersonen, Vereinen oder Clubs vergebene Namen sind nicht mit denselben Rechten bewehrt wie die digitalen „Adressen", die mit dem neuen Personalausweis erzeugt werden können. Unter den Instanzen, die im Internet Adressen vergeben, steht der deutsche Staat somit zumindest innerhalb seines Hoheitsgebiets für bestimmte im Internet getätigte Transaktionen an der Spitze dieser Hierarchie. Eine kryptographische Entsprechung fand diese Position in der Praxis der qualifizierten elektronischen Signatur, wie sie bis zur Novellierung des Signaturgesetzes im Rahmen der europäischen Harmonisierung im Jahr 2013 (vlg. die Beiträge von Bender und Hornung in diesem Band) gängig war. Mit dem Zusatz „qualifiziert" wurden im Signaturgesetz (§ 2 Absatz 3 sowie § 17 SigG) elektronische Signaturen versehen, die besondere Sicherheitsauflagen erfüllen und vor Gericht als besonders beweisfest gelten sollen, sowie in den meisten Fällen als Schriftformersatz genutzt werden können. Um qualifizierte Signaturen ausstellen zu können, mussten die Zertifizierungsdiensteanbieter dies bei der Bundesnetzagentur anzeigen (§ 4 SigG). Zusätzlich konnten sie eine Akkreditierung beantragen, in deren Rahmen die technischen und organisatorischen Abläufe des ZDA durch die Bundesnetzagentur geprüft und bestätigt wurden. Teil dieser im § 15 und § 16 des Signaturgesetzes geregelten Akkreditierung ist die Ausstellung eines sogenannten Wurzelzertifikats. Mit diesem signiert die Bun-

desnetzagentur das Schlüsselpaar des ZDA. Die Verweisungskette qualifizierter elektronischer Signaturen lief von der untersten Ebene der Bürger mit ihren individuellen Signaturkarten über die ZDA bis zur Bundesnetzagentur durch. In diesem System ist die Bundesnetzagentur gleichsam als Register der Identitätsregister mathematisch präsent und mithin eine Versinnbildlichung der Zentralisierung von Adressierungsgewalt bei der Staatlichkeit (Engemann 2011) gegeben.

Faktisch sucht der deutsche Staat also sein für die eigenen Bürger geltendes realweltliches Authentifikationsmonopol zu nutzen, um ihnen digitale Identitäten in Form des neuen Personalausweis und der krypographisch kompatiblen elektronischen Gesundheitskarte zuzustellen. Damit wird von der Staatlichkeit der Anspruch erhoben, im Internet nicht nur garantieren zu können, welche Daten zu welcher Person gehören, sondern auch gegenüber anderen Identitätsprovidern eine besonders vertrauenswürdige und geschützte Instanz zu sein.

Trotz dieses Anspruchs auf eine herausgehobene Position unter den vertrauenswürdigen Instanzen im Internet, haben diese seit 2010 real in die Brieftaschen der Bürger hineinreichenden Initiativen der deutschen Staatlichkeit wenig Wirkung gezeitigt. Die von ihr deklarierten digitalen Identitäten werden kaum angenommen. Beim neuen Personalausweises und der elektronischen Gesundheitskarte bleiben die Akzeptanz und der reale Gebrauch dieser Dokumente gering und erfüllen nicht die staatlicherseits formulierten Erwartungen. Im Vorfeld der Einführung des neuen Personalausweises gingen Vertreter des Bundesinnenministeriums beispielsweise von der Nutzung durch „80% der internet-affinen Bevölkerung aus." (Borchers 2010a, 2013). Die Gründe für deren Desinteresse und Skepsis gegenüber dem Personalausweis liegen in der mangelnde Kompatibilität und geringen Nutzerfreundlichkeit der verfügbaren Software, dem gleichzeitigem Fehlen entsprechender Angebote und Dienste bei öffentlichen Stellen (Schulzki-Haddouti 2014) sowie der initialen Kritik an der Sicherheit einzelner Komponenten (Borchers 2010b). Die private Internetwirtschaft gibt ebenfalls wenige Gelegenheiten zur Nutzung des neuen Personalausweises und begründet das mit der fehlenden Nachfrage und dem Implementierungsaufwand der vorgeschriebenen Verfahren. Bei der elektronischen Gesundheitskarte ist die Situation ähnlich. Der Gesetzgeber sah deren Einführung mitsamt einer Gesundheitstelematik genannten elektronischen Verwaltung von Patientenakten, Verschreibungen und Arztbriefen für 2006 vor. Tatsächlich wird die Karte erst seit 2011 ausgegeben, jenseits des Nachweises der Versichertendaten ist die Implementierung der Ge-

sundheitstelematik bislang nicht erfolgt. Weder ist somit die avisierte Nutzung innerhalb des Gesundheitssystems eingetreten, noch spielt dieses System für die derzeit eskalierenden Formen der körperlichen Selbstvermessung mit Gadgets wie Schrittzählern und anderen Wearables eine Rolle.

Im Vergleich zur der im ersten Teil dieses Textes beschriebenen Entwicklung im realweltlichen Raum, wo innerhalb eines Territoriums Menschen solange Freizügigkeit genießen, bis sich herausstellt, dass sie nicht identifiziert werden können, liegt derzeit mit den digitalen Ausweismedien eine andere Situation vor. Zwar hat der Staat in Deutschland für das Internet mit dem neuen Personalausweis eine neue Ausweisform geschaffen, er bindet den Zugang zu und die Bewegung in diesem Medium aber nicht an dessen Besitz oder gar Gebrauch. Das Internet ist nutzbar, ohne dass ein analoges Format zu der von Torpey für den Realraum beschriebenen staatlichen Monopolisierung der Möglichkeit der Einschränkung von Bewegungen vorliegt. Weder ist der Eintritt in diesen digitalen Raum durch Identitätsprüfungen analog zu beispielsweise Übertritten an Staatsgrenzen reguliert, noch gibt es trotz einschlägiger Regelungen beispielsweise im Urheberrecht zuverlässig wirksame Verfahren, mit denen die Bundesbürger in ihrer „Bewegungsfreiheit" oder besser Handlungsfreiheit in diesem Raum eingeschränkt werden können. Diese würden voraussetzen, dass digitales Handeln zeitnah und sicher einer bestimmten Person attribuierbar ist. Somit bleibt, trotz neuer Medien wie dem neuen Personalausweis, das digitale Handeln in Deutschland wie in den meisten westlichen Ländern bis heute tendenziell von der bürgerlichen Identität des realen Raums entkoppelt. Mit der wieder in der Diskussion befindlichen Vorratsdatenspeicherung könnten jedoch neue staatliche Kontrollformate des digitalen Raums aufkommen, die in ihrer Potenz der Zuordnung von digitalen Handlungen zu Personen schwer einzuschätzen sind.

In weniger demokratischen Ländern wie China, Russland oder dem Iran wird dagegen von staatlicher Seite massiv versucht, die Nutzung des Internets selbst und umfassend an die realweltlichen Identitätsregimes zu binden. China beispielsweise verlangt eine Registrierung mit einem amtlichen Dokument (Ansfield 2009; Lafraniere 2009; Stanley 2015), im Iran wird eine Realnamenpflicht im Internet diskutiert (Fennen 2012; Meister 2012) und Russland versucht ähnliches durchzusetzen (de Carbonnel et al. 2014; Macfarquhar 2014; Soldatov und Borogan 2015). Die tatsächliche Reichweite dieser Maßnahmen ist umstritten, sie zeigen jedoch, dass bestimmte Staaten ein dem realweltlichen Authentifikationsmonopol entsprechendes

Statut im Internet zu erreichen suchen. Einer der entscheidenden Unterschiede zu den anhand des deutschen Falles angeführten Vorhaben liegt darin, dass die Authentifikationsmechanismen nicht wie weiter unten ausgeführt als Instrumente des Datenschutzes ausgelegt sind, sondern in vielen Fällen der Erleichterung der staatlichen Überwachung dienen werden.

Ob auch liberale Demokratien langfristig nicht nur optionale Identitätsmedien für das Netz zur Verfügung stellen, sondern analog zum realen Raum im Internet anstreben, die Mittel zur Einschränkung der Handlungsfreiheit ihrer Bürger zu monopolisieren, wird sich zeigen müssen. Die digitale Vertragssicherheit, aber auch die sozialstaatliche Interventions- und Allokationsfähigkeit im und über das Internet sind auf rechtlich anerkannte digitale Identitäten verwiesen. Deren Nutzung mag in liberalen Rechtsstaaten in vielen Anwendungsfällen freiwillig bleiben, wird aber gegenüber anonymem Handeln im Falle von Rechtsstreitigkeiten Nachteile haben. Vor allem werden auch Politiker demokratischer Länder nicht müde, ein Ende der Anonymität im Internet zu fordern (A. 2014; Krempl 2011; Ramstad 2012). Der deutsche Innenminister beispielsweise hat in seinen *14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft* 2010 formuliert: „Der freie Bürger zeigt sein Gesicht, nennt seinen Namen, hat eine Adresse“ (de Maizière 2010).

3 Anonymität, Datenschutz und digitale Identität – ein paradoxes Verhältnis

Die mit solchen staatlichen digitalen Identitäten einhergehende Potenz, Handlungen im Internet eindeutig Individuen zuordnen zu können, scheint auf dem ersten Blick mit dem Datenschutz im Konflikt zu stehen. Tatsächlich ist die Situation paradox: einerseits steigern diese Verfahren das Potential der Verfolgbarkeit der Individuen, andererseits erlauben sie auch eine Stärkung des Datenschutzes aus zwei Gründen. Erstens setzt Datenschutz jenseits des Gebots der Datenminimierung voraus, dass Daten individuell zuordenbar und unterscheidbar sind. Denn die Prüfung einer Datenschutzverletzung ist auch die Prüfung der Relation zwischen Daten und Personen. Zweitens ermöglichen dieselben kryptographischen Verfahren, die bei den oben beschriebenen Medien der Identifizierung genutzt werden, die Datenverschlüsselung und feingranulierte Kontrolle der Zugriffsrechte. Im Falle der elektronischen Gesundheitskarte hat der deutsche Gesetzgeber diese Eigenschaften der Kryptographie zur Grundlage des ge-

setzlichen Forderungskataloges zur Verwaltung von Gesundheitsdaten im System der Gesundheitstelematik gemacht. Die einschlägigen Vorschriften des 5. Buches des Sozialgesetzbuches sehen ein System individualisierter elektronischer Patientenakten vor, bei dem der Versicherte den einzigen Schlüssel zu den Daten kontrolliert (Deutscher Bundestag 2004, 2015: 26). Alle Zugriffe und Operationen auf diesen Daten müssen durch den Versicherten autorisiert werden und unterliegen der Protokollierung.

Politisch wurde dieses Verfahren als „Datenhoheit beim Bürger" angepriesen und nicht nur gegenüber der deutschen Öffentlichkeit als mustergültige Implementierung des Datenschutzgedankens dargestellt. Faktisch handelt es sich um ein staatlich gewünschtes und infrastrukturell vorangetriebenes Digital Rights Management, mit dem sensible medizinische Daten geschützt werden sollen. Bislang ist die Umsetzung der bereits 2003 beschlossenen und ursprünglich für 2006 avisierten elektronischen Gesundheitskarte und dazugehörigen Gesundheitstelematik schleppend vorangekommen. Neben der Größenordnung des Vorhabens, das die Ausgabe von ca. 80 Millionen Gesundheitskarten und einer nochmals siebenstelligen (!) Zahl von komplementären Healthcare Professional Cards für Ärzte, Apotheker aber auch Pflegekräfte vorsieht (Schröder et al. 2011), gab es insbesondere von Seiten der Mediziner erhebliche Widerstände gegen dieses Projekt. Von medizinischen Fachverbänden wurde gegenüber der Öffentlichkeit vor dem „gläsernen Patienten" durch die elektronische Gesundheitskarte gewarnt. Weiterhin wurden die mit der Gesundheitstelematik einhergehenden erheblichen Veränderungen der Praxisabläufe und Abrechnungsverfahren als realitätsfern dargestellt. Letztere Kritikpunkte sind in Feldtests und Begleitforschung bestätigt worden. Bezüglich des Datenschutzes haben dagegen selbst kritische Datenschützer wie Thilo Weichert von unabhängigem Landeszentrum für Datenschutz Schleswig-Holstein betont, dass hier „eine fast ideale Realisierung der medizinischen und der informationellen **Selbstbestimmung des Patienten**" (Weichert 2009)[1] vorläge. Die Gründe für die Ablehnung seitens der Medizinerschaft sind wahrscheinlich eher in der mit der elektronischen Gesundheitskarte einhergehenden Verschiebung der Machtverhältnisse zugunsten des Patienten zu suchen (Engemann 2012a). Denn während die klassische Patientenakte aus Papier unter Kontrolle und Verwahrung der Ärzte blieb, würde zu den weiterhin in den Praxen und Kliniken geführten Behandlungsdokumenta-

1 Hervorhebung im Original C.E.

tionen die elektronische Patientenakte unter der Kontrolle der Patienten und in Verwahrung bei einem dritten Dienstleister treten. Die Kontrolle der Patientenakte soll dabei wiederum über eine Public-Key Infrastruktur gelöst werden, bei der die elektronische Gesundheitskarte des Versicherten die privaten Schlüssel vorhält. Ein Arzt muss sich gegenüber dem Patienten mittels seiner Healthcare-Professional Card ausweisen, die innerhalb der Public-Key Infrastruktur den Status des Mediziners kryptographisch abbildet. Nach Vorgaben des ursprünglichen Gesetzestextes von 2003 wäre die Entschlüsselung und der Zugriff auf eine Akte nur bei Autorisierung durch den Patienten und gleichzeitigem Nachweis der Zugriffsrechte durch den Mediziner mittels seiner Karte erfolgt. Inzwischen ist von dieser Konzeption zugunsten einer ärztegeführten Akte abgewichen worden, bei der der Patient deutlich weniger Einfluss und Einblick in das Dokumentationsgeschehen hat (Engemann 2012a). Die Karte selbst wird seit 2011 an die Versicherten ausgegeben und ist in einer technisch erneuerten Version seit 2015 zwingend als Versicherungsnachweis beim Arztbesuch vorgeschrieben. Mit dem im Dezember 2015 vom Bundestag verabschiedetem „E-Health-Gesetz“ soll die Einführung forciert werden. Der gegenwärtige Zeitplan sieht vor, die Telematikinfrastruktur zwischen 2016 und 2018 bei Praxen und Krankenhäuser einzuführen. Ab 2018 sollen Patienten einen Notfalldatensatz auf der Karte ablegen können und Ende 2018 soll eine online zugängliche elektronische Patientenakte realisiert werden. Teil des E-Health-Gesetzes ist die Öffnung der Telematikinfrastruktur und des sogenannten Patientenfaches für Daten aus Gesundheitstrackern und Wearables (Deutscher Bundestag 2015: 46).

Im Vergleich zur Konsumgüterindustrie geht die Entwicklung also langsam voran. Der Gesundheitssektor wird von der IT-Industrie als neuer Wachstumsmarkt angesehen, der insbesondere für das Internet der Dinge und Wearables attraktiv erscheint. Bereits heute werden internetbasierte Dokumentationssysteme für Körperdaten angeboten. Teil dieser Entwicklung sind neue Konstellationen zwischen medizinischer Forschung und Elektronikindustrie einerseits, IT-Unternehmen und Versicherungen andererseits. So werden im Fall der HealthKit App von Apple die anfallenden Daten explizit im Rahmen von medizinischen Studien weiter verwertet. Gleichzeitig experimentieren auch in Europa und Deutschland Versicherungen wie die Generali mit Rabatten auf Grundlage der durch Selbstaufzeichnung gewonnenen Daten. Dies entspricht der These des amerikanischen Verlegers Tim O’Reilly, dass Versicherungen das Marktmodell des Internets der Dinge werden würden, da die Risikoschätzungen der Versi-

cherungsmathematik durch die Sensordaten der Wearables auf ein neues Niveau gehoben werden könnten (Myslewski 2014). Kritiker warnen bereits vor den dystopischen Ausmaßen, die eine solchen Verkettung von staatlicher Wohlfahrt und digitaler Medienökonomie mit sich bringen könnte (Morozov 2015). In jedem Fall erwächst der von der öffentlichen Hand betriebenen ambitionierten Digitalisierung des deutschen Gesundheitssystems derzeit nicht nur privatwirtschaftlich ausgerichtete Konkurrenz, sondern die damit einhergehenden Nutzertrends schaffen möglicherweise Realitäten, denen sich die deutsche Medizin und Medizinverwaltung wie auch der Gesetzgeber werden stellen müssen. Das gilt besonders für die Standards und die Erwartungen an den Datenschutz, bei dem die privatwirtschaftlichen Akteure möglichst freien Zugriff und Weiterverarbeitung von Daten favorisieren und entsprechend mit Anreizen versehen. Von politischer Seite erhobene Forderungen, die „Nutzerdaten von Gesundheits-Apps besser zu schützen" (Bager 2015), mögen einerseits einer tatsächlicher Sorge um den Datenschutz geschuldet sein, erheben aber andererseits vor allem den Anspruch, dass dieses mit den staatlichen Authentifikationsmedien zu geschehen habe.

Grundsätzlich ist dennoch festzuhalten, dass die in Deutschland zu beobachtende Antwort auf die Krise staatlicher Authentifikationsmacht in der Realität zwar wirkungslos, im Datenschutzanspruch jedoch als progressiv einzuschätzen ist. Der neue Personalausweis und die elektronische Gesundheitskarte sollen einerseits die Zuordnung von Handlungen zu Personen und damit zu individuellen Körpern im und mit dem Internet ermöglichen, sind aber andererseits von vornherein mit der Idee der Stärkung des Datenschutzes und der Erweiterung des individuellen Kontrollbereichs von Daten gestaltet und implementiert worden. Der Slogan von der *Datenhoheit beim Bürger* ist eine treffende Fassung diese Vision, deren reale Umsetzungsfähigkeit jedoch nicht nur technische und juristische Schwierigkeiten aufwirft, sondern auch in Paradoxien führt. Denn ein kryptographisch ermächtigtes Individuum wäre in der Lage, sich nicht nur gegenüber Marktakteuren unlesbar zu machen, sondern würde im doppelten Sinne des Wortes in seinen digitalen Akten auch die Staatlichkeit von seiner Lesbarkeit ausschließen können (Scott 1998). Die elektronische Gesundheitsakte in der vom Gesetzgeber entworfenen Form wäre eine solche paradoxe Akte: Sie ist ein Dokument, das ein Versicherter bei der Nutzung der Gesundheitstelematik anlegen kann, welche aber staatliche Vertreter nur bei Einwilligung und damit Entschlüsselung durch das Individuum lesen könnten. Die elektronische Gesundheitsakte sieht nach Gesetzeslage

keine Hintertüren vor, und wenn der Versicherte die Einsicht verweigert, ist der Staat auf den Weg der Erzwingung der Herausgabe der Schlüssel verwiesen. Dies jedoch unterliegt strengen Rechtsnormierungen und ist nur im Ausnahmefall möglich. Von dieser Ausnahme abgesehen bleibt festzuhalten, dass das Beispiel der elektronischen Gesundheitsakte nach § 291a SGB V die Gleichzeitigkeit der Stiftung von Authentifizierbarkeit und Datenschutzpotenz zu zeigen vermag. Eine Potenz, die in diesem Fall soweit geht, dass die Daten sogar gegenüber demjenigen schützbar wären, der überhaupt die Mittel zur legal belastbaren Unterscheidung zwischen eigenen und fremden Daten bereitstellt: dem Staat.

4 Digitale Identität nach Snowden

Seit Edward Snowden im Sommer 2013 geheime Dokumente angelsächsischer Geheimdienste zugänglich gemacht hat, ist die Auseinandersetzung um das Verhältnis von Internet und Staatlichkeit in eine neue Phase eingetreten. Während die hier zu Tage tretenden Sachverhalte in der Öffentlichkeit hauptsächlich als unangemessen totale Überwachung skandalisiert werden (Greenwald 2014; Rosenbach, Stark 2014), kann der Blick in die vorliegenden Dokumente zeigen, wie parallel zu den bis hierher beschriebenen Projekten der Stiftung gesetzlicher digitaler Identitäten im Geheimen ebenfalls an Verfahren zur Zuordnung von Daten zu Individuen gearbeitet worden ist. Offenkundig ist die durch den Medienwandel gegebene Problemlage dieselbe, die rechtliche Situation und Interessenkonstellation eine andere: Auch Geheimdienste können nicht sicher sein, welche digitalen Interaktionen welcher Person zuzurechnen sind. Angesichts ihres Auftrages und des im mehrfachen Sinne grenzüberschreitenden Charakters ihres Tuns, können sie jedoch die Legitimationsforderungen der von ihnen mit Identitäten attribuierten Subjekte weitgehend ignorieren. Wie sich aus dem durch Snowden verfügbar gemachten Material abzuzeichnen beginnt, hatten die Geheimdienste für ihre Bedarfe das Problem der digitalen Identitäten um den Preis einer immer weiter eskalierenden Überwachung weitgehend gelöst. Denn die Stiftung von digitalen Identitäten geschieht hier nicht ex-ante im Akt der staatlichen Deklaration einer solchen, sondern relational und ex-post durch die Kompilation eingesammelter und ausgewerteter Daten zu einem individuellem Profil. Kompiliert werden diese Profile mithilfe von Selektoren. Darunter werden Suchparameter verstanden, für die ein Zusammenhang mit einer Person oder Entität vermutet werden

(Bowden 2014: 15). Dabei wird zwischen starken und schwachen Selektoren (Chamayou 2015: 5 f.) unterschieden. Erstere sind beispielsweise Telefonnummern und E-Mail-Adressen, letztere IP-Adressen oder Eigenschaftszuschreibungen wie „show me all individuals who speak German in Pakistan" (Chamayou 2015: 6). Einen Überblick des Ausmaßes solcher Selektoren gibt die 2015 veröffentlichte „Blazing Saddles" betitelte Kopie einer internen Wikipedia-Seite des britischen Geheimdienstes GCHQ (GCHQ 2015a). In diesem werden unter anderem Programme mit den Codenamen *Karma-Police*, *Marbled Gecko* und *Social Anthropoid* erläutert. Karma-Police erfasst Besuchsdaten von Webseiten und zeichnet Ort, Dauer, Korrelationen mit anderen Webseitenbesuchen sowie die IP-Adressen der Beteiligten auf. Das Programm Marbled-Gecko sammelt diese Daten für die Nutzer von Google-Earth, während Social Anthropoid alle elektronischen Interaktionsereignisse einer Instanz zusammenfassen soll (GCHQ 2015a). Solche Selektoren werden mit erheblichem technischem Aufwand unter Umgehung gesetzlicher und technischer Schutzvorrichtungen automatisiert weltweit ausgespäht und zentralisiert dauerhaft gesammelt sowie kombiniert. Für den letzteren Schritt zur Kompilation in Profilen kommen statistische Verfahren des Patternmatching, maschinelles Lernen, langfristige Beobachtungen und graphenbasierte Analysen sozialer Netzwerke zur Anwendung (Binney 2014; GCHQ 2015b; Mayer 2011). Insbesondere die Rolle von Graphenanalysen für die Zusammenfassung und Verfertigung von digitalen Identitäten aus den gesammelten Daten kann nicht überschätzt werden und ist in der bisherigen Diskussion um die Snowden-Affäre noch zu wenig beachtet worden (Chamayou 2015; Sprenger 2015). Graphen stellen Daten als Relationen von Knoten und Kanten dar und erlauben es, ihre relativen Distanzen und Zusammengehörigkeiten zu berechnen. Graphenanalysen sind Grundlage sowohl von Suchmaschinen (Röhle 2010; Rieder 2012) als auch der als Social Media bezeichneten Plattformen. Bei letzteren werden Instanzen wie Personen oder Dinge als Knoten und die Interaktionen zwischen ihnen als Kanten dargestellt (Euler 2009; Gießmann 2009; Rieder 2012). Für die Internetökonomie bilden Graphen inzwischen die entscheidende Grundlage für die Geschäftsmodelle beispielsweise von Google, Amazon und Facebook. Die Unternehmensberatung Gartner spricht in diesem Zusammenhang von fünf Graphen, die als strategische Assets fungieren: dem „Social Graph" (Facebook, Twitter), dem „Intent Graph" (Google, Ebay), dem „Consumption Graph" (Amazon), dem „Mobile Graph" (Apple, Whatsapp) und dem „Interest Graph" (Google) (Valdes 2012). Wie die angeführten Firmennamen bei

den einzelnen Graphen anzeigen, hat sich hier eine ökonomische Zentralisierung ereignet. Diese Firmen ziehen in ihren Graphen die gewaltigen Datenmengen des Big Data zusammen und werten sie aus. Mit der ökonomischen Zentralisierung geht eine Zentralisierung der dafür nötigen Medien in Form von Datencentern einher. Dabei ist es nicht allein die Masse der Daten, die dazu nötigt, große Datencenter mit immensen Rechen- und Speicherkapazitäten anzulegen; die entsprechenden Graphen weisen wie beispielsweise im Fall von Facebook Milliarden von Knoten und Trillionen von Verbindungen auf (Ching et al. 2015). Das Prozessieren von so großen Graphen in kurzer Zeit ist nicht trivial und erfordert enorme Ressourcen an Hardware und spezialisierte Software.

Die von Snowden zugänglich gemachten Dokumente wie auch eine Reihe von Interviews mit den NSA-Whistleblowern William Binney and Thomas Drake zeigen, dass die Geheimdienste ebenfalls und schon früh auf Graphenanalysen für ihre Zwecke gesetzt haben. Der früheste Hinweis findet sich noch vor Snowdens Veröffentlichungen in einem 2011 erschienen Artikel über den von der Bush-Administration angeklagten ehemaligen NSA-Beamten Thomas Drake. Dort wird Drakes Kollege und damaliger technischer Direktor der NSA William Binney folgendermaßen zitiert:

> „I wanted to graph the world." (Mayer 2011)

Drei Jahre später, im Juni 2014, wurde Binney als Zeuge im NSA-Untersuchungsausschuss des Bundestages befragt und wiederholte diese Aussage dort:

> „Wir haben einen Netzwerkgraph der gesamten Welt erstellt. Da konnten wir in einzelne Netzwerke reinzoomen und all deren E-Mails und Anrufe herausfiltern. Das hatten die damals nicht, deswegen haben sie mich danach gefragt." (Meister 2014)

Binney bezieht sich in seinen Äußerungen auf den Zeitraum zwischen Ende der neunziger Jahre und 2002, was angesichts der für einen solchen Graphen notwendigen technischen Voraussetzungen erstaunlich anmuten muss. Die von Snowden veröffentlichten Dokumente sind jüngeren Datums, bestätigen aber Binneys Aussage und die zentrale Rolle von Graphenanalysen für die Verfertigung von digitalen Identitätsprofilen. Binney selbst hat in einem Interview und einer PowerPoint Präsentation zu den Snowden-Dokumenten im Jahre 2014 noch einmal die Rolle von Graphenanalysen hervorgehoben. Unter den Codenamen PRISM, MARINA und MAINWAY betreibt die NSA graphenanalytische Programme, in die die abgehörten Kommunikationsdaten eingehen:

> „And then, once you do that, of course, you pull the data out from your-- take your graphing and then the MAINWAY MARINA program and then, when you pull this graph out and say, "I want this graph." Then you list the targets down the side. You highlight them, click, then you get a timeline of all their activity.
>
> And down on the side over here on the right, it says "Data". Well, you go to that particular point in the graph and you can pull up their email or transcribed phone call and read it. And so that's all done. This was done for profiling targets. How do they interact over time?
>
> That, by the way, can be done on anybody in the United States, because that data is in PINWALE or MARINA, or NUCLEON or both. And it's indexed.“ (Binney 2014)

Der britische Geheimdienst GCHQ betreibt ähnliche Verfahren, wie insbesondere die Präsentation mit dem Titel „„ICTR Cloud Efforts” developing “canonical” SIGINT analytics, finding hard targets and exploratory data analysis at scale“ (GCHQ 2015b) zeigt. Hier werden das Skalenniveau und die Ambitionen solcher Graphenanalysen deutlich. Die Rede ist hier von „Population-Scale“ (ibid.), und ebenso wie bei Binney wird hier selbstverständlich der Anspruch erhoben, möglichst die ganze Welt zu erfassen und Profile aus allen dem GCHQ sichtbaren auf Personen beziehbaren Daten zu schaffen: „Building Geo-Time profiles for every Internet identifier we see“. Diese sollen unter anderem zusammenfassen „how often each identifier seen in every country per week“ (ibid). Die dabei anfallenden Datenvolumina bewegen sich in Größenordnungen von „trillions of events to billions of profiles“ (ibid). Die NSA selbst hat in der Ausgabe 2/2014 ihrer öffentlich zugänglichen Vierteljahreszeitschrift „The Next Wave“ in drei Beiträgen ausführlich über die Bedeutung und technischen Herausforderungen von Graphenanalysen Auskunft gegeben (Burkhardt 2014; o. A. 2014; Rohrer et al. 2014).

Offenkundig müssen Graphen nicht nur für die Internetwirtschaft als strategisches Asset bezeichnet werden, sondern werden mindestens auch von der NSA und dem GCHQ als solche begriffen. Den sich hier abspielenden Prozess habe ich an anderer Stelle in Anlehnung an Carl Schmitts Begriff der Land- und Seenahmen als Graphennahmen (Engemann 2014: 232) bezeichnet und vermutet, dass derzeit von verschiedenen Akteuren versucht wird, „aktuellen Zugriff auf die Graphen möglichst vieler Gesellschaften und sozialer Gruppen“ zu gewinnen (ibid).

Solche mittels Graphen und im Geheimen verfertigte digitale Identitäten unterscheiden sich deutlich von den staatlicherseits öffentlich verhandelten deklarativen Identitätsformaten. Bei deklarativen Identitäten ist das

Territorium über deren Bindung an den ausgebenden Staat essentieller und über die Zeit stabiler Bezugspunkt. In Graphenanalysen sind territoriale Aufenthaltsorte ein Knoten unter anderen und gehen als immer je temporäre Geolokalisation in die dynamischen Interaktionsmuster ein. Ob jemand sich am selben Ort wie eine andere Person befinden, kann unter Umständen gegenüber ihren globalen Kontakten irrelevant sein. Wesentlich ist nicht mehr der die Lokalisation, sondern die Ordnung der Interaktionen, wie sie sich über Zeit in Graphen darstellt. Entsprechend ist in diesem Kontext eine digitale Identität die über Zeit gebildete Summe der einer Instanz zuschreibbaren Interaktionsereignisse. Das können aktive Kommunikationsvorgänge, Transaktionen oder ein simples Aufrufen von Webseiten sein, ebenso passive Interaktionen wie das automatisch stattfindende Einloggen des Handys in einer Funkzelle. Ein solches Regime unterhält eine besondere Beziehung zur Zeitlichkeit, denn die Validität der Identitätszuschreibungen schöpft sich aus dem permanenten Abgleich mit jedem neuen Ereignis im Netzwerk und dessen Passung mit dem Archiv der vorangegangen Ereignisse:

> „In the construction of the User as an aggregate profile that both is and is not specific to any one entity, there is no identity to deduce other than the pattern of interaction between partial actors.“(Bratton 2014)

Eine solche geheimdienstlich gestiftete relationale Identität ist somit eine über Zeit gewonnene und in der Zeit aktualisierte Zuschreibung, die aus einer beliebig großen Masse an anonymen, pseudonymen oder auch eindeutig einer Person zuordenbaren Selektoren extrahiert werden kann. Entsprechend unterhält ein solches Regime ein inverses Verhältnis zur Frage der Datenminimierung: Es stellt auf eine möglichst vollständige und totale Erfassung aller Daten ab, da deren Wert für das Data Mining im allgemeinen und die Zuschreibung von digitalen Identitäten im besonderen sich immer erst ex-post erweist. Die für das Tempora-Projekt des GCHQ als „Full-Take“ (Stöcker 2013) beschriebenen Absichten, den gesamten Internetverkehr aufzuzeichnen und zu speichern, können als Ausweis einer maßlosen Paranoia gelesen werden, sind aber für eine solches graphenanalytisch arbeitendes Verfahren der digitalen Identitätsstiftung sinnvoll. Jedes eingehende Datum wird auf seine Position in den Interaktionsmustern befragt und geht in die Kompilation der Profile ein. Da eine solche Kompilation gleichsam unter permanentem Falsifikationsverdacht steht und somit unabschließbar bleibt, wird die Passung dieser Profile fortwährend an neuen Daten geprüft und geschärft. Die digitalen Identitäten, die die Ge-

heimdienste für das Internet in den vergangenen zwanzig Jahren erarbeitet haben, sind nicht deklarativ zugeordnete digitale Zertifikate, deren Attribution zu einer Person auf staatliche Garantien der zugrunde liegenden Ausweisdokumente und genutzten Verfahren rekurrieren, sondern müssen als relationale Identitäten bezeichnet werden. Das von Jane Caplan für die Moderne beschriebene „reading the body" wird gleichsam um ein „reading of the relations" erweitert. Der Körper bleibt auch in diesem Zuschreibungsregime die ultimative Adresse, der im Zentrum der jeweiligen Relationen gesucht – und möglicherweise von eine Drohne ausgeschaltet – wird. Doch auch unterhalb solcher letalen Interventionen werden in einem solchen System Körper als Quellen von Handlungsketten figuriert und ultimativ in deren geo-lokalen Position gesucht. Dennoch tritt gegenüber den deklarativen Identitäten der Raum – das Hoheitsgebiet des registerführenden Staates – als Ordnungsbild in den Hintergrund und an dessen Stelle die Zeit. Einerseits im Sinne des eben beschriebenen Rekurrierens auf permanenten Datenzufluss und damit dauerhaften Registrierens, andererseits ganz medienmaterialistisch im Sinne der Potenz zur Minimierung der für die Graphenanalysen und Profilbildung notwendigen Rechenzeiten. Das beinhaltet auch und gerade die Fähigkeit, mit Supercomputern kryptographische Verfahren in vertretbaren Zeiten brechen zu können.

5 Schluss

Seit Mitte der neunziger Jahre des letzten Jahrhunderts stehen im Internet mit den deklarativen und den relationalen Identitäten zwei konkurrierende und unterschiedlich motivierte Verfahren der Zuschreibung von Identitäten in Konkurrenz. Die Zukunft von dem, was digitale Identitäten wird heißen können, wird sich nicht zuletzt über eine Klärung des Verhältnisses dieser beiden Verfahren entscheiden. Deutlich wird dies schon daran, dass graphenbasierte Metadatenanalysen die Schutzziele deklarativer digitaler Identitäten hintergehen können. Denn auch aus den Interaktionspattern verschlüsselter Kommunikation können feingranulierte Bilder sowohl des sozialen Geschehens als auch der Identitäten der beteiligten Personen extrahiert werden. Die bislang aus dem Snowden-Archiv sichtbar gewordenen Apparaturen und Organisationen stellen für die Entwicklung und Akzeptanz gesetzlich regulierter und mit entsprechenden Legitimationsansprüchen daherkommender Authentifikationssysteme erhebliche Herausforderungen dar. Schon der kursorische Blick zeigt, dass die Kompromit-

tierung kryptographischer Standards, die gezielte Unterwanderung von Infrastrukturen digitaler Authentifikation wie Trust-Centern auf der einen Seite, die die Kryptographie teilweise umgehenden Möglichkeiten der Metadatenanalyse auf der anderen Seiten die vollmundigen Versprechungen der Datenhoheit des Bürgers in Frage stellen.

Wie der zivilgesellschaftliche Forderungskatalog erweitert werden soll und kann, um etwaige Authentifikationssysteme gegenüber den Zugriffen von Geheimdiensten zu härten, ist eine offene Frage. Bislang haben sich die einschlägigen Akteure darauf konzentriert, Anonymisierungstools wie TOR und PGP zu entwickeln, sich Authentifikationsinfrastrukturen aber kaum zugewandt. In diesem Zusammenhang stellt sich insbesondere die Frage, welche Forderungen beispielsweise nach homomorphischer Verschlüsselung an die Staatlichkeit herangetragen werden müssen. Wenn die oben aufgemachte These, dass Staatlichkeit auch im Internet ein Authentifikationsmonopol anstreben wird, richtig ist, so muss dieses eingedenk der Möglichkeit drittstaatlicher Interventionen geschehen. Dass Interventionen in digitale Infrastrukturen nicht nur eine abstrakte Vorstellung sind, sondern bereits heute alltäglich stattfinden, zeigen nicht nur die von Snowden zugänglich gemachten Dokumente, sondern auch die von den USA und Israel durchgeführten Kampagnen wie Stuxnet im Iran oder die von Nordkorea veranlassten Sabotagen bei Sony Pictures. Angriffe dieser Art auf eine Authentifikationsinfrastruktur hätten weitreichende Folgen. Damit wären nicht nur Fragen des Datenschutzes und der Datenhoheit der Bürger aufgerufen, sondern darüber hinaus das Thema der Souveränität direkt berührt. Ein Souverän, der die Daten der eigenen Bürger nicht schützen kann, ist in seiner Legitimität in Frage gestellt. Die von Torpey gezeigte Monopolisierung der Einschränkung von Bewegung durch Staatlichkeit verweist außerdem auf die Frage, unter welchen Umständen ein Drittstaat einen Bürger an seiner digitalen Mobilität hindern darf. In invertierter Form ist damit aufgeworfen, dass der Staat der Garant der Bewegungsfreiheit ist, und andere Staaten oder Akteure mindestens innerhalb seines Hoheitsgebiets daran hindern muss, dass diese Einschränkungen erfährt. Im scheinbar ortunabhängigen Internet wird damit die Lokalität der Daten und der physikalische Standort ihrer Datenverarbeitungs- und übertragungsanlagen relevant. Das seit Snowden in der Datenschutzdebatte verstärkt wieder diskutierte Konzept der Data-Locality verweist darauf, denn hier wird auch für das global organisierte Cloud-basierte Computing die Verarbeitung und Speicherung der Daten innerhalb bestimmter Gebiete nachgefragt, bzw. in manchen Fällen sogar gefordert. Faktisch bedeutet

dies, dass die Bestimmung der Lokalität digitaler Transaktionen zu einem Teil der Datenverarbeitung werden müsste und das Internet das Territorium nicht transzendiert, sondern zu einer Extension desselben wird. An Stelle der vermeintlichen Ortslosigkeit von digitalen Handlungen im Internet würde eine Hyperlokalität des Handelns treten: Jede Handlung und jeder Handlungsschritt müsste auf seine geolokale Relation befragt werden. Zugleich stellt sich die Frage nach der Verortung der Graphen in gleich doppelter Weise: erstens danach wo überall Daten für Graphen gewonnen werden können – tendenziell überall –, zweitens wo die Daten zu Graphen zusammengezogen und verarbeitet werden. Es sind diese Orte, die mit den Registern der deklarativen Identitäten konkurrieren und zugleich deren Legitimitätsdimension entbehren.

Jenseits solcher Fragen nach der Widerkehr des Territorialprinzips im und gerade mit dem Internet, sollte die hier kursorisch aufgemachte Geschichte von Identitätsmedien und ihrem Wandel im Zuge der Digitalisierung zeigen, dass die digitale Identität einen Knotenpunkt der Auseinandersetzungen um Staatlichkeit und Grundordnungen im 21. Jahrhundert darstellt. Eine gesetzlich regulierte Identität, ob digital oder analog, ist nicht etwas was man hat, sondern etwas, das ein Zuschreibungsverhältnis darstellt. Wer der Dritte im Zuschreibungsverhältnis ist und mit welchen Mittel er dieses organisiert, ist eine politische Frage, die an den Kern des Staats- und Gesellschaftsverhältnisses rührt. Dabei tritt mit dem durch das Internet erzwungenen Medienwandel der Staatlichkeit die Medialitiät dieser Zuschreibungsverhältnisse in den Vordergrund und wird selbst zu einem Regierungsproblem (Engemann 2011; Sieber 2013, 2014; Schröter 2015; Engemann 2015). Vor dem Aufkommen des Internets hatten Nationalstaaten die Herstellung der Adressierbarkeit von Menschen als hoheitliche Aufgabe begriffen und in einem langen historischen Prozess entsprechende Medien und Verfahren etabliert. Das Resultat war, dass Menschen Papiere haben und von diesen Papieren ihr Status, ihre Rechte und Pflichten abhängen. In den lokalen Ausformungen unterschiedlich arbeitsteilig zwischen Staat und Markt organisiert, blieb die basale Registrierung und rechtlich wirksame Authentifikation von Menschen mittels deklarativer Identitäten ein staatliches Monopol.

Wann und wie die Bürger eine in Authentifikationsleistung und rechtlicher Belastbarkeit vergleichbare digitale Identität bekommen und ob es auch hier zu einer staatlichen Monopolisierung kommen wird, ist derzeit offen und offenkundig Gegenstand intensiver Konflikte sowohl innergesellschaftlicher als auch internationaler Natur. Ein Konglomerat von pri-

vatwirtschaftlichen Akteuren, staatliche Stellen und zivilgesellschaftliche Kräften sucht die Standards, Protokolle und Rechtsgrundlagen für die digitale Authentifikation zu beeinflussen und zu gestalten. Dabei könnte es auch zu Verschränkungen von relationalen und deklarativen Identitätsverfahren kommen, wie es beispielsweise in China diskutiert wird. Dort sollen Klarnamenprofile bei den Internetanbietern Alibaba und Tencent um ein Scoring-System erweitert werden, das beispielsweise Reiseerleichterungen vom ökonomischen und politischen Verhalten abhängig macht (Stanley 2015). Ebenso ist unklar, inwiefern in den USA im Rahmen des unter dem Titel „National Strategy for Secure Transactions in Cyberspace" (NSTIC)- Dialogs zwischen Staat, Wirtschaft und Gesellschaft relationale Identitätsformate favorisiert werden könnten. Die von der Obama-Administration angestoßene NSTIC-Strategy sieht explizit vor, ein „Identity-Ecosystem" (The White House 2011) zu schaffen, bei denen unterschiedliche Verfahren und Medien zur Authentifikation und Verwaltung von digitalen Identitäten miteinander konkurrieren sollen. Dabei wird insbesondere auf Marktkräfte vertraut: „Ultimately, the Identity Ecosystem can only be designed and built by the private sector" (The White House 2011). Große Versicherungen, Banken, aber auch Microsoft, Facebook und Google beteiligen sich aktiv am NSTIC-Prozess, und es bleibt abzuwarten, inwieweit ihre auf Graphenanalysen basierenden Verfahren in den USA in die Stiftung von auch staatlich anerkannten digitalen Identitäten eingehen. Welcher Veränderungsdruck auf das Recht von einer solchen Verschiebung von deklarativen zu relationalen Identitäten ausgehen wird, ist schwer abzuschätzen.

Die Unüberschaubarkeit der gegenwärtigen Situation wird durch die teilweise fundamentalen Widersprüche zwischen den Akteuren weiter erschwert. Das gilt insbesondere auf internationaler Ebene, wo neben den unterschiedlichen Pfadabhängigkeiten, Rechtstraditionen und politischen Systemen aus dem gesamten Spektrum von autokratischen bis liberal-demokratischen Staaten bereits heute Konflikte digital ausgetragen werden. Die durch Snowden unternommenen Veröffentlichungen lassen keinen Zweifel daran, dass dabei sowohl die Identifikation von Menschen als auch die Kompromittierung von digitalen Infrastrukturen ebenso Alltagsgeschäft der Geheimdienste ist, wie die Versuche für sämtliche Populationen Graphen zu erstellen.

Trotz dieser unübersichtlichen Lage und der Differenzen zwischen den genannten Interessenträgern, ist ihnen gemeinsam, dass sie weder an einem anonymen Internet noch an einer Fortsetzung des derzeitigen Status

quo Interesse haben. Die Interessen der Privatwirtschaft, staatlicher Akteure und von staatlichen Geheimdiensten kreuzen sich in der aus jeweils unterschiedlichen Interessen motivierten Notwendigkeit, Menschen im Netz dauerhaft und sicher erkennen zu können – wirtschaftliche Akteure aus Gründen der Vertragssicherheit, aber auch Mittels der Profilbildung Käufer und Absatzchancen einschätzen zu können (Bratton 2014; Bernard 2016; Wichum 2016), staatliche Akteure aus den genannten Notwendigkeiten der Rechtsicherheit, Strafverfolgung, wohlfahrtsstaatlichen Allokation und Partizipationsformaten an der öffentlichen Verwaltung. Wie der deutsche Fall beispielsweise bei der Gesundheitskarte zeigt, kann die Motivation auch darin bestehen, eine Datenschutzagenda voranzutreiben und auf ein kryptographisch solideres Fundament zu stellen.

Die Geheimdienste schließlich suchen digitale Spuren Personen zu attribuieren. Als in der Staatenkonkurrenz aktive Agenten ist ihre Aufgabe dabei, auch den eigenen Selbstauskünften nach, digitale Ereignisse Personen zuordnen zu können (Friedman, Wagoner 2015). Mit den dabei entstandenen Formaten relationaler Identitäten treten sie in Konflikt mit den Ansprüchen auf das Authentifikationsmonopol der von ihnen überwachten Staaten.

An der digitalen Identität spannen sich so gleich eine ganze Reihe von Paradoxien auf, die insbesondere liberale Rechtsstaaten verhandeln müssen. Die Paradoxien umfassen den gleichberechtigten Anspruch auf Identität und Anonymität, auf Sicherheit und das Recht allein gelassen zu werden, und auf Schutz der digitalen Freizügigkeit bei gleichzeitigem staatlichem Anspruch auf deren Einschränkung unter bestimmten Bedingungen. Tragfähige Kompromisse für diese Dilemmata werden sich angesichts der geschilderten Konstellationen und Schwierigkeiten nur schwierig und in einem internationalen Aushandlungsprozess finden lassen. Hier zeichnet sich bereits eine Eskalationslinie der zeitgenössischen Gouvernemedialität ab, bei der die Frage nach den Medien der Selbstverhältnisse und der politischen Relationsgefüge mehr und mehr zum Gegenstand gesellschaftlicher Auseinandersetzung wird.

Literatur

Ambrosi, Christine (2014): „Überwachung und das Recht auf Anonymität im Internet: Anmerkungen zur Lateinstunde mit Thomas de Maizière“, *netzpolitik.org*, https://netzpolitik.org/2014/ueberwachung-und-das-recht-auf-anonymitaet-im-internet-anmerkungen-zur-lateinstunde-mit-thomas-de-maziere/.

ACLU (2015): „NSA Documents“, *American Civil Liberties Union*, https://www.aclu.org/nsa-documents-search.

Ansfield, Jonathan (2009): „China Web Sites Seeking Users' Names“, *The New York Times*. 6.9.2009.

Bager, Jo (2015): „Unionsfraktion will Nutzerdaten in Gesundheits-Apps besser schützen“, *heise online*, http://www.heise.de/newsticker/meldung/Unionsfraktion-will-Nutzerdaten-in-Gesundheits-Apps-besser-schuetzen-2811793.html.

Beavan, Colin (2001): *Fingerprints. The Origins of Crime Detection and the Murder Case that launched Forensic Science*, New York: Hyperion.

Bernard, Andreas (2016): „Profil – Erfassung – Selbstdesign“, in: Weich, Andreas (Hrsg.): *Profile: Individualisierung, Kollektivierung und Klassifizierung durch Daten*, Lüneburg: Meson Press, i.E.

Binney, William (2014): „Retired NSA Technical Director Explains Snowden Docs“, *alexaobrien.com*, http://www.alexaobrien.com/secondsight/wb/binney.html.

Borchers, Detlef (2013): „Der ePerso hat Geburtstag: Drei Jahre neuer Personalausweis“, *heise online*, http://www.heise.de/newsticker/meldung/Der-ePerso-hat-Geburtstag-Drei-Jahre-neuer-Personalausweis-2037387.html.

Borchers, Detlef (2010a): „ePerso liefert Anscheinsbeweis bei Online-Bestellung“, *heise online*, http://www.heise.de/newsticker/meldung/ePerso-liefert-Anscheinsbeweis-bei-Online-Bestellung-1150484.html.

Borchers, Detlef (2010b): „Neuer Personalausweis: AusweisApp mit Lücken [2. Update]“, *heise online*, http://www.heise.de/newsticker/meldung/Neuer-Personalausweis-AusweisApp-mit-Luecken-2-Update-1133376.html.

Bowden, Caspar (2014): *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens' fundamental rights*, Brüssel: Policy Department Citizens' Rights and Constitutional Affairs.

Bratton, Benjamin (2014): „The Black Stack“, in: *e-flux*. 53.

Brin, David (1998): *The Transparent Society. Will Technology force us to choose between Privacy and Freedom*, New York, NY: Basic Books.

Burkhardt, Paul (2014): „Big Graphs“, in: *The Next Wave* 20 (4), 11–19.

Buschmann, Arno (2014): *Mit Brief und Siegel. Kleine Kulturgeschichte des Privatrechts*, München: C.H. Beck.

Caplan, Jane (2001): „„This or That Particular Person“: Protocols of Identification in Nineteenth-Century Europe“, in: Torpey, John und Caplan, Jane (Hrsg.): *Documenting Individual Identity the Development of State Practices in the Modern World*, Princeton, New Jersey: Princeton University Press, 49–66.

Caplan, Jane und Torpey, John (Hrsg.) (2001): *Documenting Individual Identity the Development of State Practices in the Modern World: the development of state practices in the modern world*, Princeton, New Jersey: Princeton University Press.

de Carbonnel Alissa, Teterevleva Anastasia und Kiselyova Maria (2014): „Russia demands Internet users show ID to access public Wifi“, *Reuters*. 8.8.2014.

Chamayou, Grégoire (2012): *Manhunts. A philosophical history*, Princeton and Oxford: Princeton University Press.

Chamayou, Grégoire (2015): „Oceanic Enemy. A brief philosophical history of the NSA“, in: *RadicaL Philosophy* 191 (May/June 2015), 2–12.

Ching Avery, Edunov Sergey, Kabiljo Maya et al. (2015): „One trillion edges: graph processing at Facebook scale“, http://www.vldb.org/pvldb/vol8/p1804-ching.pdf.

Cole, Simon A (2001): *Suspect Identities*, Cambridge Massachusetts: Harvard University Press.

Corwin, Philip, S. (1998): „Electronic Authentication: The Emerging Federal Role“, in: *Jurimetrics* 38 (3), 261–275.

Covell Paul, Gordon Steve, Hochberger Alex, et al. (1998): *Digital Identity in Cyberspace*, Boston, Mass: Massachusetts Institute of Technology.

Cryptome (2015): „Snowden release tally“, https://cryptome.org/2013/11/snowden-tall y.htm.

Derrida, Jacques (2005): „Paper or Me, You Know... (New Speculations on a Luxury of the Poor)“, in: *Paper Maschine*, Stanford: Stanford University Press, 41–65.

Deutscher Bundestag (2015): *Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen*.

Deutscher Bundestag (2004): *Gesetz zur Modernisierung der gesetzlichen Krankenversicherung*.

Engemann, Christoph (2015): „Die Adresse des freien Bürgers: Digitale Identitätssysteme Deutschlands und der USA im Vergleich“, in: *Leviathan - Berliner Zeitschrift für Sozialwissenschaft* 43 (1), 43–63.

Engemann, Christoph (2012a): „Elektronische Gesundheitsakte oder Fallakten – Medizinische Archivmacht und die elektronische Gesundheitskarte“, in: Kray Ralph, Koch Christoph und Sawicki, Peter T. (Hrsg.): *Qualität in der Medizin dynamisch denken: Versorgung - Forschung - Markt*, Berlin, Heidelberg: Springer Verlag, 149–175.

Engemann, Christoph (2014): „Human Terrain System: Soziale Netzwerke und die Medien militärischer Anthropologie“, in: Baxmann Inge, Beyes Timon und Pias Claus (Hrsg.): *Soziale Massen - Neue Medien*, Berlin - Zürich: Diaphanes, 205–230.

Engemann, Christoph (2011): „Im Namen des Staates: Der elektronische Personalausweis und die Medien der Regierungskunst“, in: *Zeitschrift für Medien- und Kulturforschung* (2), 211–228.

Engemann, Christoph (2012b): „Write Me Down Make Me Real. Zur Gouvernemedialität der digitalen Identität“, in: Passoth, Jan-Hendrik und Wehner, Josef (Hrsg.): *Quoten, Kurven und Profile – Zur Vermessung der Gesellschaft*, Wiesbaden: VS Verlag für Sozialwissenschaften, 205–230.

Engemann, Christoph und Traue, Boris (2006): „Governmediality of the Life Course“, *governmediality.net*, governmediality.net.

Euler, Leonard und Velminski, Wladimir (Hrsg.) (2009): *Die Geburt der Graphentheorie*, Berlin: Kadmos.

Fennen, Nicolas (2012): „Iran: Aufbau eines staatlichen E-Mail-Systems“. *netzpolitik.org*, https://netzpolitik.org/2013/iran-aufbau-eines-staatlichen-e-mail-systems/.

Friedman, Arthur R. und Wagoner, Larry D. (2015): „The Need for Digital Identity in Cyberspace Operation“, in: *Journal of Information Warfare* 14 (2), 42–52.

Froomkin, A. Michael (1995): „The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution“, in: *University of Pennsylvania Law Review* 143 (3), 709–897, DOI: 10.2307/3312529.

GCHQ (2015a): „Blazing Saddles“, https://fveydocs.org/document/blazing-saddles/.

GCHQ (2015b): *ICTR Cloud Efforts" developing "canonical" SIGINT analytics, finding hard targets and exploratory data analysis at scale*, London: ICTR, GCHQ.

Gießmann, Sebastian (2009): „Graphen können alles. Visuelle Modellierung und Netzwerktheorie vor 1900“, in: *Visuelle Modelle*, München: Fink Verlag, 269–284.

Granville Edge, Major Percy (1928): „Vital Registration in Europe. The Development of Official Statistics and some Differences in Practice“, in: *Journal of the Royal Statistical Society* 91 (3), 346–393.

Greenwald, Glenn (2014): *Die globale Überwachung. der fall Snowden, die amerikanischen Geheimdienste*, München: Droemer.

Groebner, Valentin (2004): *Der Schein der Person - Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters*, München: C.H. Beck.

Hertel Christian, Jickeli Joachim, Knothe, Hans-Georg et al. (Hrsg.) (2004): *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen*, Berlin: Walter de Gruyter.

Hornung, Gerrit (2005): *Die digitale Identität. Rechtsfragen von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren*. Baden-Baden: Nomos.

Hull, Matthew S (2012): *Government of Paper. The Materiality of Bureaucracy in Urban Pakistan*, Berkeley: University of California Press.

Kahn, David (1996): *Codebreakers. The Story of Secret Writing*, New York, NY: Scribner.

Kantorowicz, Ernst (1957): *The King's Two Bodies. A Study in Mediaeval Political Theology*, Princeton N.J.: Princeton University Press.

Kittler, Friedrich A. (2012): „„And the Gods made Love.“ Zum Tode von Cornelia Vismann“, in: Hamacher, Werner und Kittler, Friedrich A. (Hrsg.): *Das Schöne am Recht*, Berlin: Merve Verlag, 43–48.

Krempl, Stefan (2011): „Debatte über Anonymität und Pseudonyme im Netz dauert an“. *heise online*, http://www.heise.de/newsticker/meldung/Debatte-ueber-Anonymitaet-und-Pseudonyme-im-Netz-dauert-an-1351355.html.

Kubicek, Herbert und Noack, Thorsten (2010): *Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich*, Berlin: LIT Verlag.

Lafraniere, Sharon (2009): „Name Not on Our List? Change It, China Says“, *The New York Times*, 21.4.2009.

Langenbach, Christian J. und Ulrich, Otto (2002): *Elektronische Signaturen Kulturelle Rahmenbedingungen einer technischen Entwicklung*, Berlin, Heidelberg: Springer Verlag.

Macfarquhar, Neil (2014): „Russia Quietly Tightens Reins on Web With 'Bloggers Law'", *The New York Times*, 6.5.2014.

de Maizière, Thomas (2010): „14 Thesen zu den Grundlagen einer gemeinsamen Netzpolitik der Zukunft", http://www.bmi.bund.de/cae/servlet/contentblob/1099988/publicationFile/88667/thesen_netzpolitik.pdf.

Mayer, Jane (2011): „The Secret Sharer Is Thomas Drake an enemy of the state?", in: *The New Yorker*, 23.5.2011.

Meister, Andre (2012): „Internet-Zensur im Iran: „Sauberes" nationales Intranet statt Internet", *netzpolitik.org*, https://netzpolitik.org/2012/internet-zensur-im-iran-sauberes-nationales-intranet-statt-internet/.

Meister, Andre (2014): „Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: „Größte Bedrohung der Demokratie seit US-Bürgerkrieg"", *netzpolitik.org*, https://netzpolitik.org/2014/live-blog-4-anhoerung-im-nsa-untersuchungsausschuss/.

Morozov, Evgeny (2015): „A dystopian welfare state funded by clicks", http://evgenymorozov.tumblr.com/, http://evgenymorozov.tumblr.com/post/126030163570/a-dystopian-welfare-state-funded-by-clicks.

Müller, Lothar (2012): *Weisse Magie. Die Epoche des Papiers*, München: Carl Hanser Verlag.

Myslewski, Rik (2014): „The Internet of Things helps insurance firms reward, punish". *The Register*, http://www.theregister.co.uk/2014/05/23/the_internet_of_things_helps_insurance_firms_reward_punish/.

Noriel, Gerhard (2001): „The Identification of the Citizen: The Birth of Republican Civil Status in France", in: Torpey, John und Caplan (Hrsg.): *Documenting Individual Identity*, New Jersey: Princeton University Press, 28–48.

o. A. (2014): „Globe at a Glance: The Graph500 Top 11 Supercomputers", in: *The Next Wave* 20 (4), 37–38.

Opitz, Sven (2012): *An der Grenze des Rechts. Inklusion/Exklusion im Zeichen der Sicherheit*, Weilerswist: Velbrück Wissenschaft.

Ramstad, Evan (2012): „South Korea Court Knocks Down Online Real-Name Rule", *Wall Street Journal*. 24.8.2012.

Rieder, Bernhard (2012): „What is in PageRank? A Historical and Conceptual Investigation of a Recursive Status Index.", in: *Computational Culture a journal of software studies* 2.

Röhle, Theo (2010): *Der Google-Komplex. Über Macht im Zeitalter des Internets*, Bielefeld: Transcript Verlag.

Rohrer Randall, Lyn Paul Celeste und Nebesh, Bodan (2014): „Visual analytics for Big Data", in: *The Next Wave* 20 (4), 20–37.

Rosenbach, Markus und Stark, Holger (2014): *Der NSA-Komplex: Edward Snowden und der Weg in die totale Überwachung*, München: DVA.

Salter, Mark B (2003): *The Passport In International Relations*, Boulder: Lynne Rienner Publishers.

Schröder Klaus Theo, Schladweiler Dirk, Tschoepe Sven et al. (2011): „Bericht der Arbeitsgruppe der Gesellschafterversammlung zur vorgezogenen Lösung für die Telematikinfrastruktur und einen stufenweisen Ausbau“, http://www.dkgev.de/media/file/10721.RS456-11_Anlage-SGBV_291a_GSV_A.pdf.

Schröter, Jens (2015): „Das mediale Monopol des Staates und seine Verteidigungslinien“, in: *Zeitschrift für Medien und Kulturforschung* 6 (2), 13–25.

Schulzki-Haddouti, Christiane (2014): „Bundesländer für elektronischen Rechtsverkehr nicht ausreichend vorbereitet“, *heise online*, http://www.heise.de/newsticker/meldung/Bundeslaender-fuer-elektronischen-Rechtsverkehr-nicht-ausreichend-vorbereitet-2394718.html.

Scott, James C. (1998): *Seeing Like a State. How Certain Schemes to Improve the Human Condition Have Failed*, New Haven: Yale University Press.

Seutter, Konstanze (1996): *Eigennamen und Recht*, Tübingen: May Niemeyer Verlag (Reihe germanistische Linguistik).

Sieber, Samuel (2013): „Die Medialität des Politischen und die Politiken der Medien. Fragmente und Fugen (medialen) Mit-Seins“, in: *Interventionen. Festschrift für Georg Christoph Tholen*, Marburg: Schüren, 295–306.

Sieber, Samuel (2014): *Macht und Medien: zur Diskursanalyse des Politischen*, Bielefeld: Transcript Verlag (MedienAnalysen).

Siegert, Bernhard (2003): *Passage des Digitalen - Zeichenpraktiken der neuzeitlichen Wissenschaften 1500-1900*, Berlin: Brinkmann und Bose.

Siegert, Bernhard (2006): *Passagiere und Papiere. Schreibakte auf der Schwelle zwischen Spanien und Amerika*, München: Wilhelm Fink Verlag.

Siegert, Bernhard (1993): *Relais. Geschicke der Literatur als Epoche der Post 1751 - 1913*, Berlin: Brinkmann und Bose.

Siegert, Bernhard und Vogl, Joseph (2003): *Europa. Kultur der Sekretäre*, Berlin Zürich: diaphanes.

Singh, Simon (1999): *Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet*, München: Hanser.

Soldatov, Andrei und Borogan, Irina (2015): *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, New York: PublicAffairs.

Sprenger, Florian (2015): *The Politics of Micro-Decisions*. meson press.

Stanley, Jay (2015): „China's Nightmarish Citizen Scores Are a Warning For Americans“. *American Civil Liberties Union*, https://www.aclu.org/blog/free-future/chinas-nightmarish-citizen-scores-are-warning-americans.

Stöcker, Christian (2013): „GCHQ Surveillance: The Power of Britain's Data Vacuum“. *Spiegel Online*, http://www.spiegel.de/international/world/snowden-reveals-how-gchq-in-britain-soaks-up-mass-internet-data-a-909852.html.

Tantner, Anton (2007): *Ordnung der Häuser, Beschreibung der Seelen: Hausnummerierung und Seelenkonskription in der Habsburgermonarchie*, Innsbruck, Wien, Bozen: Studienverlag.

The White House (2011): *National Strategy for Trusted Identities in Cyberspace (NSTIC)*, Washington DC.

Torpey, John (1998): „Coming and Going: On the State Monopolization of the Legitimate „Means of Movement““, in: *Sociological Theory* 16 (3), 239–259.

Torpey, John (2000): *The Invention of the Passport*, Cambridge: Cambridge University Press.

Valdes, Ray (2012): „The Competitive Dynamics of the Consumer Web: Five Graphs Deliver a Sustainable Advantage“. *Gartner*, https://www.gartner.com/doc/2081316/competitive-dynamics-consumer-web-graphs.

Vismann, Cornelia (2000): *Akten - Medientechnik und Recht*. Frankfurt am Main: Fischer Verlag.

Weber, Max (2002): *Wirtschaft und Gesellschaft Grundriß der verstehenden Soziologie*, 5. rev. Auflage, Tübingen: Mohr.

Weichert, Thilo (2009): *Stellungnahme zur elektronischen Gesundheitskarte anlässlich der öffentlichen Anhörung des Gesundheitsausschusses am 25. Mai 2009, Anträge der Fraktionen FDP und BÜNDNIS 90/DIE GRÜNEN*. Berlin.

Wichum, Ricky (2016): *Biometrie. Zur Soziologie der Identifikation*, München: Wilhelm Fink Verlag.

Die zitierten Webseiten wurden im April 2016 letztmalig auf ihre Aktualität überprüft.

Digitale Identifizierung

Johannes Eichenhofer / Christoph Gusy[1]

1 Von der digitalen Identität zur digitalen Identifizierung

„Identität“ ist ein großes Wort. Der Vielzahl seiner Verwendungen entspricht eine Vielzahl von Deutungen und Bedeutungen. Zu denken ist etwa an die „europäische Identität“ oder die Identitäten in Europa: die nationale („Identität der Deutschen“), religiös-kulturelle („jüdische Identität in Europa“), Ein- und Auswanderer-Identitäten („Siedler-Identität“), die „Identität des Selbst“ und die „soziale Identität“ in Gesellschaften – sei es als trennende oder gemeinsame Identität. Psychologie, Soziologie, Ethnologie und Pädagogik suchen nach Erscheinungsformen und Herstellungsmöglichkeiten von Identität (Überblick: Eickelpasch und Rademacher 2004). Identität wird überall gesucht und gefunden. Darin liegen ihre Größe und ihr Dilemma. Denn immer neu stellt sich heraus: „Identisch“ ist ein Phänomen nur mit sich selbst. Genau danach fragt die *digitale Identität*: Ist die Person, mit der ich digital kommuniziere, dieselbe wie diejenige Person, mit der ich früher kommunizierte? Oder dieselbe, für die sie sich ausgibt? Oder dieselbe, die ich kenne? Es geht um deren Identifizierbarkeit. Das ist einerseits weniger als „Identität“, andererseits aber gewisser als bloße Identitätskonstrukte. Und noch wichtiger: Für die Zwecke der digitalen Kommunikation ist sie ausreichend.[2]

---

1 Für vielfältige Hinweise und freundliche Unterstützung danken wir Frau Prof Dr. Sandra Seubert, Herrn Prof. Dr. Rüdiger Grimm, Frau wiss. Mit. Laura Schulte sowie den übrigen Kolleginnen und Kollegen aus dem Projekt „Strukturwandel des Privaten“ (www.strukturwandeldesprivaten.de).

2 Nicht Gegenstand des Beitrags sind folglich die soeben genannten, in der Psychologie, Soziologie, Ethnologie, Pädagogik oder im Verfassungsrecht thematisierten internen Leistungen eines Menschen zur Herausbildung seiner eigenen „Identität“ im Sinne des eigenen Selbst, wie z.B. die Selbstdefinition und Selbstverwirklichung und die aufgrund dieser Prozesse nach außen gerichtete Selbstdarstellung (vgl. hierzu instruktiv Britz 2007).

Sobald einander unbekannte Personen miteinander kommunizieren,[3] kann auf Seiten mindestens eines Kommunikationsteilnehmers das Bedürfnis entstehen, sich über die „Identität“[4] der anderen Teilnehmer zu vergewissern (Hornung 2005: 29). Dies gilt jedenfalls dann, wenn die andere Person in der Lage ist, die eigenen Interessen zu beeinträchtigen. Im Zivilrecht wird diesem Bedürfnis beispielsweise bei der Begründung von Dauerschuldverhältnissen Rechnung getragen, wenn Vertragsverhältnisse nicht einfach unter Anwesenheit begründet und abgewickelt werden oder im Rahmen der Feststellung von zustell- oder ladungsfähigen Anschriften. Daher schreibt das Bürgerliche Gesetzbuch (BGB)[5] für den Abschluss besonders folgenreicher Rechtsgeschäfte die Wahrung einer bestimmten Form zwingend vor (vgl. §§ 125 ff. BGB) und verpflichtet dadurch jede Vertragspartei – etwa durch die im Rahmen der Schriftform (§ 126 BGB) notwendige Unterschrift oder durch die Verwendung einer elektronischen Signatur – die eigene Identität zu offenbaren (sog. Identitätsfunktion der Unterschrift – vgl. dazu Ellenberger 2014: 109; zur elektronischen Signatur Bösing 2005).[6] Ein Bedürfnis nach Identitätsfeststellung kann sich aber auch im Staat-Bürger-Verhältnis ergeben, etwa wenn eine Leistungs- oder sonstige Anspruchsberechtigung überprüft werden soll, wenn eine Person unter dem Verdacht steht, eine Straftat begangen zu haben (vgl. § 163b Abs. 1 der Strafprozessordnung – StPO)[7] oder wenn sie sich auch nur an einem besonders gefährlichen oder gefährdeten Ort aufhält (vgl. etwa § 12 Abs. 1 Nr. 2 und 3 des nordrhein-westfälischen Polizeigesetzes – PolG

3 Zum Begriff der Kommunikation: Kloepfer 2002: 27; Vesting 2012: 17 ff.

4 Unter „Identität“ soll im Folgenden lediglich die Einzigartigkeit und aufgrund dessen die Unterscheidbarkeit einer Person verstanden werden, woraus sich die Möglichkeit der Feststellung ihrer Authentizität (Echtheit) ergibt (vgl. zum Begriff der Authentizität, insbesondere zu Verfahren ihrer Feststellung: Hornung, in Hornung und Möller 2011: 2; Hornung 2005: 79 ff.).

5 Bürgerliches Gesetzbuch v. 18.8.1896 in der Fassung der Bekanntmachung vom 2.1.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 1 des Gesetzes vom 22.7.2014 (BGBl. I S. 1218).

6 Zu Recht betont Bizer (2003: 83) aber, dass es im Zivilrecht für das Wirksamwerden einer Willenserklärung unerheblich ist, „ob ihr Urheber sie unter seinem wirklichen Namen abgegeben hat.“ Zudem steht nach § 13 Abs. 6 TMG jedermann das Recht zu, im Internet unter einem Pseudonym aufzutreten (dazu Spindler 2012: 84 f., 120 f.).

7 Strafprozessordnung vom 1.2.1877 in der Fassung der Bekanntmachung vom 7.4.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 Abs. 3 des Gesetzes vom 21.1.2015 (BGBl. I S. 10).

NRW).[8] Auch die in § 1 des Personalausweisgesetzes (PAuswG)[9] niedergelegte Pflicht eines jeden mindestens 16 Jahre alten Bürgers, einen Personalausweis zu besitzen[10] und diesen gemäß § 1 Abs. 1 S. 2 PAuswG auf Verlangen einer berechtigten öffentlichen Behörde vorzulegen, soll dem staatlichen Bedürfnis nach „Identitätsvergewisserung" dienen. Nachweisen kann eine Person ihre Identität im Wesentlichen aufgrund von drei Merkmalen (vgl. Hornung 2005: 29): (1) dem *Besitz* bestimmter Legitimationspapiere (z.B. Personalausweise), (2) dem *Wissen* um bestimmte Informationen (z.B. eine PIN)[11] und (3) dem bloßen *Sein*, d.h. aufgrund bestimmter biologischer Merkmale wie Fingerabdrücken, Stimme, Iris oder DNA-Spuren (vgl. hierzu Albrecht 2003). Die Identitätsfeststellung ist primär auf die Erkenntnis ausgerichtet, bestimmte Merkmale über eine Person zu erfahren (z.B. den Namen), um diese Person für bestimmte Zwecke zu einem späteren Zeitpunkt kontaktieren und aufsuchen zu können. In einem weiteren Sinne soll die Identitätsfeststellung die Feststellung ermöglichen, dass die betroffene Person die bereits über sie bekannten Merkmale aufweist. So kann etwa im Rahmen einer polizeiliche Identitätsfeststellung[12] überprüft werden, ob der Adressat der Maßnahme die in seinem Personalausweis genannten Merkmale (z.B. Größe, Alter, Augenfarbe) tatsächlich aufweist. Mit dieser Feststellung ist jedoch ein überaus geringer Erkenntnisgewinn verbunden. Vor allem setzt sie voraus, dass über eine Person bereits bestimmte Merkmale bekannt sind, woran es in der Praxis bisweilen fehlt – wenn den Behörden etwa kein Legitimationspapier oder eine sonstige Möglichkeit eines Identitätsnachweises (Besitz, Wissen, Sein) zur Verfügung steht. In diesen Fällen ist die *Identifizierung* des Betroffenen erforderlich.

Identifizierung zielt im Gegensatz zur Identitätsfeststellung auf die Bestimmung der Identität einer unbekannten Person, wenn es gerade an

---

8 Polizeigesetz des Landes Nordrhein-Westfalen in der Fassung vom 25.6.2003, zuletzt geändert durch Art. 2 des Gesetzes vom 8.7.2003 (GVBl. NRW S. 410).

9 Personalausweisgesetz vom 18.6.2009 (BGBl. I S. 1346), zuletzt geändert durch Art. 2 Abs. 13 und Art. 4 Abs. 1 des Gesetzes vom 7.8.2013 (BGBl. I S. 3154).

10 Demgegenüber begründet das PAuswG keine Pflicht einen Personalausweis *mit sich zu führen* – so ausdrücklich (wenn auch zur Vorgängerregelung): Hornung 2005: 48 mwN. Siehe zur aktuellen Regelung: Möller in Hornung und Möller 2011, § 1 PAuswG Rn 3 ff.

11 Dieser Möglichkeit des Identitätsnachweises kommt im Internet bisher die größte Bedeutung zu.

12 Vgl. hierzu etwa Gusy 2014: 123 ff.

einem der vorbenannten Identitätsnachweise fehlt. In diesem Falle werden diejenigen bereits bekannten Merkmale einer Person mit unbekannter Identität mit den Merkmalen einer Person mit bereits bekannter Identität verglichen. In diesem Sinne bedarf die Identifizierung also bestimmter Informationen und sie generiert selbst neue Informationen. Auf diesem Verfahren der Identifizierung basieren moderne Datenbanken.[13] Hier werden die über eine Person bekannten Attribute bzw. Eigenschaften zu einem sog. „Datensatz" zusammengefasst. Die Datensätze werden dann im Hinblick auf die Attribute durch ein sog. Relationsschema unterschieden. Zusätzlich wird jede Person mit einem sog. Schlüssel versehen, der dann die eindeutige Identifizierung im Sinne einer Wiedererkennung[14] ermöglicht. Vor allem können verschiedene Tabellen (z.B. das Melderegister und das Bundeszentralregister) miteinander verbunden werden. Mit dieser Vorgehensweise ist dann ein Mehrwert an Information und Erkenntnis verbunden: So kann beispielsweise von einem Autokennzeichen auf den Halter und dessen Wohnort geschlossen werden. Ziel der Identifizierung ist also nicht allein der Abgleich einer zu überprüfenden Person im Hinblick auf bestimmte Eigenschaften (z.B. Größe, Alter oder Augenfarbe) mit einen *bereits vorliegenden* Referenzdatensatz (z.B. den in einem Personalausweis aufgeführten Daten), sondern zuvor und zumindest auch die *Ermittlung des Referenzdatensatzes* aus einer großen Menge von Referenzdaten (vgl. Hornung in Hornung und Möller 2011: 2; Hornung 2005: 79 f.). Allerdings setzt das Verfahren der Identifizierung voraus, dass Klarheit über die Eigenschaft besteht, anhand derer die Verknüpfung zwischen den Tabellen hergestellt werden kann.[15] Die Lösung zur Überwindung dieses

13 In der Praxis werden vor allem „relationale Datenbanken" zur Identifizierung eingesetzt. „Relationale Datenbanken" sind Sammlungen von Tabellen (= den sog. Relationen). Diese setzen sich wiederum aus sog. Tupeln / Zeilen zusammen, die auch als „Datensatz" bezeichnet werden. Jedes dieser Tupeln setzt sich nun aus einer Vielzahl von Attributen bzw. Eigenschaften zusammen, die in der Tabelle als Spalten ausgedrückt werden. Das sog. Relationsschema drückt nun das Verhältnis von Tupeln / Zeilen und Attributen / Spalten aus. Vertiefend: Meier 2007: 4 ff. Daneben werden aber auch andere Datenbankenvarianten wie Graphdatenbanken, Linked-Lists oder NOSQL zur Identifizierung eingesetzt.

14 Die Unterscheidung zwischen der auf *Erkenntnis* gerichteten Identitätsfeststellung und der auf *Wiedererkenntnis* gerichteten Identifizierung geht zurück auf Dreier 1987: 1014.

15 Dieses Problem bezeichnet Druey (1995: 59 ff.) als „sekundäres Informationsbedürfnis", das er wie folgt beschreibt: „... Information (ist) gleichsam ein Fass ohne Boden: ihre Verfügbarkeit schafft beim Subjekt sogleich das Bedürfnis nach weite-

Problems kann entweder darin bestehen, immer mehr Daten über die vorgefundene und die gesuchte Person zu erheben, zu speichern und auszuwerten. Diese Lösung kann jedoch aus verschiedenen Gründen nicht überzeugen: Sie würde letztlich zu einer unendlichen Datenerhebung führen, was aus rechtlichen Gründen nicht zulässig wäre.[16] Eine andere Lösung besteht darin, die Eigenschaften, nach denen gesucht werden soll – mithin die Vergleichsmaßstäbe – einseitig (d.h. hoheitlich) festzulegen. Allerdings müssen diese Maßstäbe, um reproduzierbar und damit für eine Vielzahl von Identifizierungsvorgängen anwendbar zu sein, ein gewisses Maß an Verallgemeinerung bzw. Abstraktion zulassen. Auch hier stellt sich dann aber letztlich wieder das von der Identitätsfeststellung bekannte Problem, dass die für die Identifizierung zuständige Behörde nicht nur die maßgeblichen Merkmale bzw. Kriterien der gesuchten und der vorgefundenen Person, sondern auch die Kriterien für die Maßgeblichkeit eines Vergleichsmaßstabs kennen muss. Allerdings sind derartige Kriterien notwendig unvollständig. Empirische Studien zeigen, dass selbst „biometrische Systeme" wie z.B. DNA-Analysen die Identifizierung einer Person nicht zu 100% realisieren können (vgl. Albrecht 2003: 52 ff.). Reduziert werden kann die Wahrscheinlichkeit eines sog. „false-non-match" durch die Erhebung von Zusatzinformationen. Problematisch hieran ist aber, dass es diese Informationen oftmals entweder gar nicht gibt, oder dass sie nicht (verlässlich) ermittelt werden können. Dieses Problem stellt sich angesichts der zunehmenden Mobilität der Menschen und der grundsätzlichen Möglichkeit der Fälschung von Informationen immer dringlicher. Gerade die Erhebung von „fälschungssicheren" Informationen kann nur durch die Erhebung von Zusatzinformationen sichergestellt werden. Trotz dieser Probleme wurden im Laufe der letzten Jahre der neue Personalausweis und die elektronische Gesundheitskarte eingeführt und in diesem Kontext der Aufbau einer „Informationsinfrastruktur" (Gusy 2012: 155) bzw. „Identifizierungsinfrastruktur" (Hornung 2005: 7, 321) eingeleitet.

---

rer Informationen." Vor allem „wird das neue Bedürfnis im Fall der Information nicht als subjektive Reaktion geschaffen, sondern liegt in der Sache selbst. Die Beurteilung jeden Sachverhalts und die Bestimmung des dadurch gebotenen Verhaltens erfordert unbeschränkte Information.".

16 Dazu unten IV. Vor diesem Hintergrund erweist sich der Einsatz von Big-Data-Technologie, die auf einer potentiell unendlichen Datenverarbeitung basiert, als rechtlich problematisch. Zu den Rechtsfragen von „Big Data" etwa Strandburg 2014: 5 ff.; Hoeren (Hrsg.) 2014.

2 Digitale Identifizierung

Wie soeben gesehen, verknüpft Identifizierung bislang bekannte und verteilte Informationen über eine Person und generiert hierdurch neue Informationen und Erkenntnisse über diese Person. Hier schafft der Einsatz des Internet sowohl quantitativen wie auch qualitativen Wandel. Erstens werden immer mehr personenbezogene Daten (im Sinne von § 3 Abs. 1 des Bundesdatenschutzgesetzes – BDSG)[17] in das Netz gestellt und dadurch bestimmten Identifizierungsinfrastrukturen zugänglich gemacht (Spindler 2012: 73).[18] Zweitens: Sind diese Daten einmal in das Internet eingespeist, so lassen sie sich nur schwer und kaum je überall wieder löschen. Auch wenn in jüngerer Zeit die Forderung nach einem „Recht auf Vergessenwerden" erhoben (vgl. etwa Mayer-Schönberger 2011: 199 ff.; abwägend Spindler 2012: 35 f., 85 ff.; Hornung und Hofmann 2013: 163 ff.) und dieses Schutzbedürfnis vom EuGH[19] anerkannt wurde, sind einmal online gestellte Daten – rein technisch gesehen – jederzeit wieder abrufbar. Ein Grund für den Bedeutungszuwachs der Identifizierung in Zeiten des Internets liegt darin, dass sich die Identität einer Person im Internet schwieriger feststellen lässt als in der realen Welt. Schließlich lassen sich in einer analogen face-to-face-Kommunikation äußere Merkmale (Aussehen, Mimik, Gestik, Stimmführung u.a.) des Kommunikationspartners ohne weiteres feststellen, woraus wiederum Schlüsse auf seine Identität gezogen werden können.[20] Analoge Kommunikation ist so gleichsam multimedial; sie

17 Bundesdatenschutzgesetz vom 20.12.1990 in der Fassung vom 14.1.2003 (BGBl. I S. 66), zuletzt geändert durch Art. 1 des Gesetzes vom 14.8.2009 (BGBl. I S. 2814). Nach § 3 Abs. 1 BDSG sind „personenbezogene Daten ... Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffener)." Strittig ist, ob IP-Adressen „personenbezogene Daten" im Sinne von § 3 Abs. 1 BDSG darstellen – vgl. dazu etwa Schild 2013: § 3 Rn 21 mwN. Diese Frage stellt sich auch im Hinblick auf den Begriff der „personenbezogenen Daten" nach Art. 2 lit. a) der EU-Datenschutz-RL 95/46/EG. Der Bundesgerichtshof (BGH) hat mit Beschluss v. 28.10.2014, Az. VI ZR 135/13, dem Europäischen Gerichtshof (EuGH) diese Frage zur Vorabentscheidung vorgelegt, der hierüber jedoch noch nicht entschieden hat – vgl. EuGH Rs. C-582/14 – *Breyer*.

18 Zu erinnern sei etwa an den digitalen Personalausweis oder die elektronische Gesundheitskarte – vgl. hierzu Hornung 2005: 37 ff., 131 ff.

19 EuGH, Rs. C-131/12 – Google Spain, Rn 89 ff.

20 Hierin liegt auch der Grund, weshalb etwa zur Feststellung der Identität einer Leiche die Verwandten derjenigen Person gebeten werden, den die zuständigen Behörden für den Verstorbenen halten.

schafft Nähe und dadurch zugleich die Überprüfbarkeit kommunizierter Informationen. Man kann – mit mehr oder weniger Geschick oder Ausbildung – sehen oder hören, ob jemand lügt. Aber genau diese Überprüfbarkeit setzt zugleich Nähe voraus; eine Nähe, die ihrerseits durch Kommunikation geschaffen wurde. Davon unterscheidet sich digitale Kommunikation zwar nicht notwendigerweise, wohl aber regelmäßig. Die virtuelle Welt führt auch Personen zusammen, die einander entweder gar nicht kennen oder nur über wenige Informationen voneinander verfügen. Die durch das Internet bewirkte Vernetzung (potentiell) aller mit dem Netz verbundenen Endgeräte (d.h. Computer, Smartphones, Tablets etc.; perspektivisch viele Alltagsgegenstände) und die hierdurch zugleich geschaffene Möglichkeit der Kommunikation, d.h. des Transfers von Daten zwischen den Endgeräten[21] erweist sich vor allem dann als reizvoll, wenn eine face-to-face-Kommunikation gerade nicht möglich oder nicht sinnvoll erscheint.

Damit verbunden ist nun aber das Problem, dass die in das Internet eingespeisten Informationen keineswegs wahr sein müssen. Vielmehr kann die „digitale Identität" einer Person von dieser selbst oder von Dritten entwickelt, verändert und ggf. gefälscht werden, wodurch Informationen ihrer Bedeutung beraubt werden können: „On the internet, nobody knows you're a dog."[22] Zwar setzt jeder Datentransfer zwischen einem Informationen und Leistungen bereitstellenden „Server"-Rechner und einem Informationen und Leistungen beziehenden „Client"-Rechner die *Authentifizierung* des Clients durch den Server voraus.[23] Dies geschieht, indem der Client dem Server seine IP-Adresse[24] übermittelt. Auf diese Weise kann ein Server „in Erfahrung bringen", welches Endgerät das betroffene Datenpa-

---

21 Beziehungsweise: Den auf den Endgeräten installierten Programmen – auf die Notwendigkeit diese Präzisierung macht Sievers (2003: 38) aufmerksam.

22 So ein berühmter Cartoon von *Peter Steiner* in: The New Yorker, 5.7.1993, welcher zwei sich vor dem Computer amüsierende Hunde zeigt.

23 Vgl. etwa Weidner-Braun 2012: 57. Zum Begriff der Authentizität bereits oben (Fn 4).

24 Bei einer IP (Internet Protocol)-Adresse handelt es sich um eine (in der aktuell immer noch ganz überwiegend verwendeten Version IPv 4) 32bit lange nach binärem Schema gewährleistete Zahlenkommunikation. Sie dient der eindeutigen Identifikation eines jeden Rechners (nämlich des Adressaten des Datentransfers) im Internet, was dadurch gewährleistet wird, das jede IP-Adresse zu einem gegebenen Zeitpunkt nur einem Rechner zugewiesen wird – vgl. Weidner-Braun 2012: 62.

ket von ihm anfordert.[25] Die Authentifizierung lässt jedoch lediglich den Schluss darauf zu, welches Endgerät ein Datenpaket anfordert und ermöglicht im Gegensatz zur *Identifizierung* nicht den Schluss auf den (unbekannten) *Nutzer* des Endgerätes.[26] Zwar kennt das Internet verschiedene Möglichkeiten des Identitätsnachweises, wobei vor allem das „Wissen" in Gestalt von Passwörtern und PIN von großer Bedeutung ist. Die Aussagekraft dieser Formen des Identitätsnachweises darf aber bezweifelt werden. Zum einen besteht die Möglichkeit, dass sich ein Dritter unbefugt das Passwort oder die PIN des Betroffenen verschafft hat und sich nun als dieser ausgibt. Zum anderen können die im Internet versandten Datenpakete von Dritten unbefugt abgehört, abgefangen, manipuliert, umgeleitet oder mit einer gefälschten IP-Adresse versehen werden (sog. IP-spoofing).[27]

Digitale Kommunikation steht also vor folgendem Grundproblem: Die Partner digitaler Kommunikation sind in Distanz, und sie bleiben auch in Distanz. Und jedenfalls bis in die Gegenwart hinein ist ihre Kommunikation über Chats, E-Mails u.ä. unimedial oder jedenfalls nicht derart multimedial wie die face-to-face-Kommunikation. Damit bleiben die gerade aus der Multimedialität der face-to-face-Kommunikation begründeten Überprüfungsmöglichkeiten von Informationen hier (noch) ausgesperrt. Die kommunikativ begründete Nähebeziehung ist hier also zumindest eine qualitativ andere als in traditionellen Kommunikationsbeziehungen. Sie ist eine rein informationelle Nähe. Im Übrigen können aber die Überprüfungsmöglichkeiten jedenfalls bis in die Gegenwart hinein nur aufgrund weiterer Informationen überprüft werden. Einerseits ist das Internet in der Lage, Informationen mit einem größeren syntaktischen[28] Gehalt zu transportieren, als dies in der analogen Welt möglich wäre. Andererseits haben die im Internet veröffentlichten Informationen aber einen geringeren se-

25 Schaar (2014: 71 f.) macht zudem darauf aufmerksam, dass der Server auch einsehen kann, „welches Betriebssystem, welcher Browser dort installiert, welche Sprach- und Grafikeinstellungen jeweils aktiviert sind." Zu den damit verbundenen Problemen des „Browser-Fingerprinting" s. den Beitrag von Herrmann und Federrath in diesem Band.

26 So auch Sievers 2003: 75: „Aus der notwendigen Verwendung von IP-Adressen ergibt sich ... nicht zwangsläufig Kenntnis von der Identität seiner Benutzer (...)".

27 Vgl. zu diesen „protokollimmanenten Angriffsmöglichkeiten": Hobert 1998: 52 ff.

28 Die syntaktische Dimension einer Information beschreibt eine Information in ihrer Eigenschaft als Zeichengebilde aus Text, Bildern oder Tönen (vgl. Druey 1995: 7; Kloepfer 2002: 24 f.).

mantischen[29] Wert als solche, die im Rahmen einer herkömmlichen face-to-face-Kommunikation ausgetauscht werden.[30] Vor diesem Hintergrund erweist sich die Kommunikation im digitalen Raum als in höherem Maße *distanziert*. Sie setzt Distanz voraus und stabilisiert auch ein höheres Maß an Distanz, solange sie eine digitale Kommunikation bleibt. Diese Grundannahme muss nicht für alle Zeiten so bleiben. Solange die Übertragungskapazitäten noch nicht erschöpft und die Miniaturisierung der Hardware noch Raum lässt, können sich in Zukunft hier die Verhältnisse ändern. Bis in die Gegenwart hinein ist der Befund jedoch realistisch.

3 Distanz im Netz: Ausgangspunkte digitaler Kommunikation

Das Ziel, den digitalen Bürger digital identifizieren zu wollen, erweist sich zumindest als anspruchsvoll, wenn nicht gar als selbstwidersprüchlich. Denn einerseits setzt die Kommunikation im Internet Distanz zwischen den Kommunikationsteilnehmern voraus.[31] Andererseits verlangt Identifizierung traditionell nach Nähe, also dem Abbau dieser Distanz. Ein Ausweg aus diesem Dilemma wird in der Suche nach Wiedererkennungs- und Fälschungssicherheit gesehen. Das Ziel staatlicher Identifizierungsbemühungen ist also primär eine Annäherung an unverfälschbare Daten. Die größte Gewähr hierfür scheinen gegenwärtig biometrische Merkmale (besonders unterscheidungskräftig: DNA- oder die Irismerkmale) einer Person zu bieten (Albrecht 2003: 48 ff.). Die Verifizierung von Informationen über eine Person ist also auf die Erhebung weiterer, für die Identität eines Menschen besonders prägender und insofern höchstpersönlicher Merkmale angewiesen. Dadurch verringert sich nun die Distanz zwischen der Per-

---

29 Die semantische Dimension einer Information bezeichnet „den Vorgang der Kodierung bzw. Dekodierung beim Sender bzw. beim Empfänger, d.h. der Transferierung von Sinn und Zeichen und umgekehrt." (vgl. Kloepfer 2002: 24 f.; ebenso: Druey 1995: 7).

30 In diesem Sinne *Paul Watzlawick*: „Digitale Kommunikationen haben eine komplexe und vielseitige logische Syntax, aber eine auf dem Gebiet der Beziehungen unzulängliche Semantik. Analoge Kommunikation dagegen besitzen dieses semantische Potenzial, ermangeln aber der für eindeutige Kommunikationen erforderlichen Syntax." (Watzlawick et al. 2011: 78).

31 Dasselbe gilt im Übrigen für die Telekommunikation. Bereits der Begriff setzt sich zusammen aus dem griechischen „tele" (fern) und dem lateinischen „communicare" (gemeinsam tun / machen) (Kleih 2010: 28).

son und den Identifizierungsmerkmalen: Je sicherer die Wiedererkennung sein soll, desto höchstpersönlicher sind die zu erhebenden / speichernden / verarbeitenden Daten. Identifizierungsbemühungen haben also zwangsläufig ein Eindringen in die Persönlichkeit des Bürgers zur Folge. Diese These soll nun anhand von drei Problemfeldern veranschaulicht werden.

Erstens: Das Internet eröffnet besonders vielfältige Möglichkeiten der *multivariablen Datennutzung*. Dort verfügbare Informationen über einen Bürger kann eine staatliche Stelle – jedenfalls rein faktisch[32] – prinzipiell in jeder Situation und zu jedem Zweck aufrufen oder an weitere staatliche Behörden weiterleiten. Datenerhebung heißt aber immer auch: Herauslösung eines Datums aus seinem Zusammenhang („Dekontextualisierung"). Datenverarbeitung bedeutet, das Datum in einen neuen Zusammenhang einzuführen („Rekontextualisierung"). Es ist jedoch bekannt, dass mit jeder Re-Kontextualisierung ein Informationsverlust einhergeht.[33] Der betroffene Bürger kann also leicht „in falsches Licht gerückt werden" und sich hiergegen nur schwer wehren (Worms und Gusy 2012: 93).[34] Damit ist, *zweitens*, das Problem der sog. *Beweislastverschiebung* angesprochen: Zwar können Informationen im Netz nicht einfach als wahr gelten. Aber auch dort gilt vielfach die Vermutung, wonach kein Rauch ohne Feuer entstehen kann. Dies gilt umso mehr, je vielfältiger, konkreter und höchstpersönlicher die Informationen sind – unabhängig davon, wer sie ins Netz gestellt hat. Betroffene Personen müssen dann oftmals große Anstrengungen unternehmen, um die Indizwirkung der über sie veröffentlichten Informationen zu widerlegen. Jeder Mensch läuft im Internet also Gefahr, auf seine „Netzidentität" reduziert und so verzerrt zu werden, ohne dass er auf diesen „Datenschatten" Einfluss hätte (Worms und Gusy 2012: 95 f.).

---

32 In rechtlicher Hinsicht gilt für den Staat das sog. Zweckbindungsgebot: Informationen dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden (vgl. § 14 Abs. 1, § 28 BDSG; siehe auch: Gusy 2011: 139; Hornung 2005: 157 ff.). Demgegenüber soll nach Auffassung des BVerfG die sog. „Online-Streife", d.h. die Kenntnisnahme und Erhebung von öffentlich zugänglichen Informationen durch die Polizeibehörden, keinen Grundrechtseingriff darstellen, solange hierbei nicht gezielt nach einer bestimmten Person gesucht und Informationen über sie zusammengetragen werden – vgl. BVerfGE 120, 274, 344 f.. Kritisch dazu: Oermann und Staben 2013: 638.

33 Gemeint ist hier die Information in ihrer semantischen Dimension (s.o., Fn 29).

34 Hieran wird deutlich, dass eine Informationsverarbeitung in Form der Rekontextualisierung einen eigenständigen, meist schwerwiegenden Grundrechtseingriff darstellt (Gusy 1983: 102 ff.; 2011: 96 f.).

Dann tritt der Datenschatten kommunikativ an die Stelle der Person selbst – sie wird zur bloßen Resultante ihres Schattens. Das ist keine Grenze informationeller Selbstbestimmung; das ist vielmehr ihr genaues Gegenteil. Nicht das Selbst bestimmt die Information, sondern die Information macht das soziale Selbst. Hieran zeigt sich *drittens*, dass bei im Internet veröffentlichten Informationen eine besonders hohe *Gefahr ihres Missbrauchs* besteht. Ein Missbrauch durch staatliche Stellen kann in einer Nichtbeachtung des Zweckbindungsgebotes liegen. Dann werden Informationen zu anderen Zwecken verarbeitet als zu denjenigen, zu welchen sie erhoben wurden. Andererseits kann die Sicherung bestimmter Informationen gegen Missbrauch – z.B. durch Verschlüsselungstechniken[35] – gerade dazu führen, dass die Informationsmengen, die eine sicherere Identifizierung ermöglichen könnten, begrenzt werden. Hier geraten dann Informationssicherheit und Identifizierungssicherheit in einen Widerspruch.

4 Distanz als Faktum und als rechtliches Gebot am Beispiel des Staat-Bürger-Verhältnisses

Distanz erschwert Identifizierung, schließt sie aber nicht notwendig aus. Diese bedarf aber besonderer digitaler Mittel. Sie alle – Distanz, Identifizierung und dazu notwendige Mittel – sind rechtlich relevant. Nur wie? Gibt es ein rechtliches Distanzgebot?

Ein solches ließe sich zunächst von der Prämisse einer fundamentalen *Trennung von Staat und Gesellschaft* her formulieren. Während sich diese Vorstellung – als Reaktion auf den allumfassenden Staat des Absolutismus – im 19. Jahrhundert noch großer Beliebtheit erfreute, besteht heute weitgehend Einigkeit darüber, dass Staat und Gesellschaft zwei sich wechselseitig überschneidende und aufeinander bezogene Verbände darstellen. Einerseits nimmt der Staat als „organisierte politische Entscheidungseinheit" Aufgaben für die Gesellschaft wahr. Andererseits bedient er sich als „organisierte Wirkeinheit" menschlicher Träger (vgl. Böckenförde 1972: 395, 405 ff.) in einer anderen Rolle, nämlich als Staatsvolk. Beide – Volk und Gesellschaft – sind namentlich im demokratischen Verfassungsstaat vielfältig aufeinander bezogen und eben nicht „getrennt". Daher kann jene

35 Vgl. zur Funktionsweise derartiger Verschlüsselungsverfahren etwa Gerhards 2010: 30 ff.

Trennung auch nicht als Grundlage eines vom Staat gegenüber seinen Bürgern zu wahrenden Distanzgebotes herangezogen werden.

Ein weiterer Ansatzpunkt für die Ermittlung eines solchen Distanzgebotes wäre das sog. „*forum internum*“: Es ist anerkannt, dass jeder Bürger das Recht hat, seine Gedanken, Meinungen, Anschauungen und religiösen Überzeugungen frei zu bilden. In dieses *forum internum*“ darf der Staat nicht eingreifen (vgl. etwa Di Fabio 2001: 164 ff.). Staatliche Eingriffe sind vielmehr erst dann zulässig, wenn sich die Gedanken, Meinungen, Anschauungen oder religiösen Überzeugungen als „*forum externum*“ nach außen manifestieren. Da sich das *forum internum* aber nicht nur jedem Eingriff, sondern auch dem Zugriff des Rechts insgesamt entzieht (Worms und Gusy 2012: 93), kann es auch kein rechtliches Distanzgebot begründen. Zudem ist digitale Identifizierung ein kommunikationsbezogener und -gestützter Prozess in einer Situation, in welcher relevante Informationen das *forum internum* längst verlassen haben.

Allerdings lässt sich möglicherweise auf Grundlage der sog. „*Sphärentheorie*“ ein Distanzgebot entwickeln. Die vom Bundesverfassungsgericht zur Konkretisierung des „allgemeinen Persönlichkeitsrechts“ aus Art. 2 Abs. 1 und Art. 1 Abs. 1 GG entwickelte (vgl. BVerfGE 27, 344, 351; E 33, 367, 376 f.; E 80, 367, 373 ff.) Sphärentheorie (hierzu: Britz 2007: 6 ff., 37 ff.; Di Fabio 2001: 160 ff.; Dreier 2013: 376 ff.; Gusy 2003: 103 ff.; Worms und Gusy 2012: 93 f.) soll das Persönlichkeitsrecht in mehr und weniger schutzbedürftige Sphären unterteilen und dadurch Öffentliches und Privates voneinander abgrenzen (Worms und Gusy 2012: 93 f.). Bereits in seiner frühen Rechtsprechung hat das Bundesverfassungsgericht jedem Bürger einen „unantastbaren Bereich privater Lebensgestaltung“ zuerkannt, „der der Einwirkung der öffentlichen Gewalt entzogen ist“ (vgl. BVerfGE 6, 32, 41). Inzwischen differenziert das Bundesverfassungsgericht zwischen einer besonders schutzbedürftigen und deshalb unantastbaren Intim-, einer ebenfalls schutzbedürftigen Privat- und einer weniger geschützten Öffentlichkeitssphäre (vgl. Gusy 2003: 103, 104 ff.). Abgegrenzt werden die Sphären anhand äußerer Merkmale, d.h. einerseits räumlich und andererseits in thematischer Hinsicht.[36] Eingriffe in die Intimsphäre, die dem „Bereich privater Lebensgestaltung“ entspricht und de-

36 Vgl. BVerfGE 120, 180, 199: „In thematischer Hinsicht betrifft“ der Bereich privater Lebensgestaltung „insbesondere Angelegenheiten, die von dem Grundrechtsträger einer öffentlichen Erörterung oder Zurschaustellung entzogen zu werden pflegen. In räumlicher Hinsicht gehört zur Privatsphäre ein Rückzugsbereich des

ren Verwirklichung für die Menschenwürde (Art. 1 Abs. 1 GG) unentbehrlich ist, sollen danach nie zulässig sein (vgl. etwa Di Fabio 2001: 161). Dies hat allerdings zur Folge, dass sich aus der Intimsphäre – wie schon aus dem „forum internum" – kein Distanzgebot begründen lässt, da sich die Intimsphäre nicht nur als staats-, sondern auch als „rechtsfreier Raum" erweist (Gusy 2003: 105). Etwas anderes gilt für die Privatsphäre, die sich von der Intimsphäre „in ihrem Sozialbezug" unterscheidet (Di Fabio 2001: 162) und kein Element der Menschenwürde enthält (vgl. Gusy 2003: 107). Eingriffe in diese Sphäre sind daher grundsätzlich zulässig, allerdings nur zur Wahrung überragend wichtiger Güter des Gemeinwohls (BVerfGE 32, 373, 380 f.). Kern der Privatsphäre ist das Recht des Einzelnen, frei darüber zu entscheiden, ob er eine Information geheim halten oder diese der Öffentlichkeit preisgeben möchte (Gusy 2003: 106). Vor diesem Hintergrund kann aus der Privatsphäre ein Distanzgebot dahin abgeleitet werden, dass der Staat nicht befugt ist, Informationen über Bürger gegen deren Willen zu erheben. Dabei muss es sich um Informationen handeln, die der Privat- und nicht der Öffentlichkeitssphäre zuzuordnen sind, da letztere ohnehin durch Beobachtung wahrgenommen oder kommunikativ ermittelt werden können (Gusy 2003: 108).

Damit ist das vom Bundesverfassungsgericht anerkannte *Recht auf informationelle Selbstbestimmung* (grundlegend: BVerfGE 65, 1 ff.) angesprochen, welches sich von der Sphärentheorie dahin unterscheidet, dass die Abgrenzung zwischen Privatem und Öffentlichem nicht als äußerlich vorgegeben betrachtet wird. Vielmehr soll der Bürger selbst entscheiden können, ob er eine Information als „privat" ansieht und deshalb für sich behalten möchte oder ob er sie nach außen preisgibt und damit zu erkennen gibt, dass er sie als öffentlich ansieht (Worms und Gusy 2012: 94, 96). Ein Eingriff in dieses Recht liegt demnach vor, wenn der Bürger vom Staat gezwungen wird, Informationen preiszugeben, die er eigentlich für sich behalten wollte. Unabhängig von der Frage, ob der Bürger angesichts der oben (III.) dargestellten Problemfelder die vom Recht auf informationelle Selbstbestimmung vorausgesetzte Möglichkeit hat, das Schicksal „seiner" Daten zu beherrschen, führt dieser Ansatz Freiheit und Informationsbeherrschung zusammen. Doch ist seine Reichweite in der realen, vermachteten Gesellschaft begrenzt. Hier schlägt Selbstbestimmung allzu

---

Einzelnen, der ihm insbesondere im häuslichen, aber auch im außerhäuslichen Bereich die Möglichkeit des Zu-Sich-Kommens und der Entspannung sichern.".

rasch in Fremdbestimmung um. Zudem enthält der Selbstbestimmungsansatz kaum Lösungen für den Fall, dass die Daten bereits an Dritte gelangt sind. Aufgrund dessen wird das Recht auf informationelle Selbstbestimmung zuweilen auch als „illusionär" und „lebensfremd" bezeichnet.[37]

Schließlich ließe sich ein Distanzgebot aus dem in der *Menschenwürde* (Art. 1 Abs. 1 GG) wurzelnden Recht auf Kenntnis der eigenen Identität bzw. der identitätskonstruierenden Merkmale herleiten. So hat das Bundesverfassungsgericht etwa ein Recht auf Kenntnis der eigenen Herkunft (BVerfGE 38, 241, 251 ff.) und Abstammung anerkannt (BVerfGE 90, 263). Diese Rechte sind allerdings ihrer Schutzrichtung nach weniger auf die Abwehr staatlicher Identifizierungsversuche gerichtet, sondern betreffen eher die Herausgabe von identitätskonstruierenden Merkmalen. Sie sind daher keine Grundlage für ein Distanzgebot.

Damit ist festzuhalten, dass sich ein Distanzgebot jedenfalls zwischen Staat und Bürger am ehesten als theoretischer Ausgangspunkt und in Kommunikationsverhältnissen nur unter fallbezogenen Differenzierungen begründen lässt:[38] Der Staat ist danach nicht befugt, sich sämtliche, für ihn nützliche Informationen von seinen Bürgern zu beschaffen. Vielmehr ist seine *Informationserhebung auf das Notwendige beschränkt*. Umgekehrt wird ein absoluter, für den Staat unübersteigbarer Kernbereich des Privaten (krit. aber Dammann 2012) und der Kenntnis der Bürger hinsichtlich der eigenen Identität anerkannt. Deren Umschreibung ist aber bislang allenfalls im Ansatz gelungen. Dies ergibt sich schon allein aus der Frage, was alles zum Recht auf eine eigene Identität gehört; die rechtskulturellen Grundlagen und Grenzen (etwa zum Fingerabdruck als Identifikationsmerkmal) sind noch in der Diskussion. *Limitiert ist auch die staatliche Verarbeitung erhobener Daten*: Sie dürfen nicht zu allen, sondern nur zu bestimmten Zwecken verwendet werden.[39] Beide Limitierungsgebote sind

37 Vgl. Bull 2011: 46. Kritische Anmerkungen zum Selbstbestbestimmungsansatz finden sich insbesondere auf S. 34 und 42.

38 Siehe zur Daseinsberechtigung der Sphärentheorie neben dem Recht auf informationelle Selbstbestimmung auch: Gusy 2003: 112 ff.

39 Siehe zu diesem Zweckbindungsgebot bereits oben, Fn 32. Nach Auffassung des BVerfG ist eine gesetzliche Regelung, die vorsieht, Daten auf Vorrat zu speichern, um sie später zu einem bestimmten Zweck einzusetzen, indes nicht grundsätzlich verfassungswidrig – vgl. BVerfGE 125, 260, 316. „Strikt verboten" sei lediglich „die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken" – vgl. BVerfGE 125, 260, 317; zuvor bereits: BVerfGE 65, 1, 46; E 100, 313, 360.

aber, um Wirksamkeit zu entfalten, auf ihre prozedurale Absicherung angewiesen.

Einerseits gilt: Digitaler Rechtsverkehr bedarf der digitalen Identifizierung. Wer die Vorteile des ersteren nutzen will, wird die Nachteile der letzteren hinnehmen müssen. Insbesondere das grundsätzliche rechtliche Distanzgebot wird ein weiteres Mal relativiert. Dabei geht es um mehr und anderes als neue Formen von In- und Exklusion. Dies ist nicht per se gut oder schlecht. Doch es geht um die Bedingungen und Instrumente der Inkludierbarkeit; um die Möglichkeit von Kontrolle und Transparenz auch für Kunden und Endnutzer. Der „Schleier des Nichtwissens“[40] eint die Community immer weniger, er trennt vielmehr allzu oft Anbieter und Nachfrager, Kunden und Unternehmen, Laien und Experten, Nichtwissende und Wissende. Wer Selbstbestimmung will, bedarf eines Mindestmaßes an Information über Grundlagen und Folgen seines Handelns. Allerdings treten rechtliche Gleichheit der Benutzer und tatsächliche Ungleichheit ihrer Benutzung ein weiteres Mal auseinander. Wo sich derart neue Asymmetrien auftun, sind Freiheit, freier Wettbewerb und Vertragsgerechtigkeit nicht einfach da, sondern rechtlich herzustellen und ggf. durchzusetzen. Netz und Netzgemeinde bedürfen der Legitimation durch neue Offenheit. Rechtliche Vorgaben und technische Identifizierungsstrukturen müssen dem Rechnung tragen. Dialog über Prämissen und Grenzen tut hier Not.

5 Vom Wandel der Problemlagen zum Wandel des Rechts?

Anderseits gilt: Digitale Identifizierbarkeit und Identifizierungsinfrastrukturen unterliegen also nicht nur faktisch, sondern auch rechtlich dem Problem der Distanz. Während die Vielfalt der Menschen (potentiell) unbegrenzt ist, sind den Möglichkeiten ihrer Identifizierbarkeit/Wiedererkennbarkeit (rechtliche) Grenzen gesetzt. Wie gesehen hängt der Verlauf dieser Grenzen davon ab, was heute als öffentlich und was als privat gilt. Hier sind im Hinblick auf die Maßstäbe („Was ist heute öffentlich, was ist privat?“), die Wirkungen („Was ändert sich eigentlich?“) und die Bewertung („Ist das gut oder schlecht?“) noch viele Fragen offen. Fest steht jedoch, dass die zunehmende Digitalisierung und Vernetzung der Bürger zu einer

40 Das Bild des „veil of ignorance“ geht zurück auf den amerikanischen Philosophen *John Rawls*, dem es als Grundlage seiner „Theorie der Gerechtigkeit“ diente – vgl. Rawls 1979: 29 ff.

Ausdehnung der Öffentlichkeitssphäre zulasten der Privatsphäre geführt hat (Worms und Gusy 2012: 95), und zwar erst recht, wenn und wo die Menschen auf Kommunikation im Netz angewiesen sind. Doch ist es für Verschwindensdiagnosen und Niedergangsszenarien (vgl. etwa Heller 2011) gewiss zu früh. Vielmehr stellt sich die Situation als technische und rechtliche Herausforderung. „Privatheit" erscheint mehr denn je als rechtlich herzustellendes und technisch organisationsbedürftiges ultimum refugium libertatis – nicht nur als Rückzugsraum, sondern als Grundlage einer freien und demokratischen Gesellschaft!

Das Recht steht also offensichtlich an einem Scheideweg. Im digitalen Rechtsverkehr stellt sich nicht die Alternative von Distanz oder Identifizierung. Beides ist notwendig: Es geht um Identifizierung unter den Bedingungen von Distanz. Hier müssen Instrumente und Rechtsformen entwickelt werden.

Hier findet der Kampf manchmal noch an der falschen Front statt. Als Beispiel mag hier die Idee der *Vernetzung* stehen. An die Stelle der älteren Identifikation mithilfe großer *Referenzdateien*[41] tritt die Vernetzung einzelner Datenverarbeitungsstellen, etwa im Pass- oder Personalausweiswesen (§§ 22a PassG, 25 PAuswG). Vernetzung führt dazu, dass es statt einem „großen Bruder" viele „kleine Brüder" gibt, die aber zusammen nicht minder effektiv sind als der alte Große. Das Internet prägt zudem ein *Paradigma der Asymmetrie*: Die Vorteile des Netzes sind unmittelbar und gegenwärtig, der Preis – in Informationen entrichtet – ist unsichtbar und zumeist erst später bemerkbar: Im Staat des „e-government" (hierzu: Britz 2012) und erst recht im Wirtschaftsverkehr des „e-commerce" mit seinen Allgemeinen Geschäftsbedingungen reduziert sich allzu oft die informationelle Selbstbestimmung auf die Zustimmungslösung. Und wer zugestimmt hat, hat seine Selbstbestimmung nicht verloren, sondern ausgeübt![42] Schließlich ist noch auf ein weiteres Problem hinzuweisen, das hier als *Paradigma der Verfügbarkeit* bezeichnet werden soll: Wie bereits gesehen (III.), eröffnet Digitalisierung die technische Möglichkeit, einmal erhobene Daten in praktisch jedem anderen Zusammenhang einzusetzen. So dient etwa die Scheckkarte der Alterskontrolle und der Fingerabdruck

41 Damit ist gemeint, dass einzelne Datensätze mit einer zentralen Referenzdatei (z.B. einem Melderegister) abgeglichen werden.

42 Das Problem verschärft sich noch angesichts der festzustellenden „zunehmenden Oligopolisierung" im Netz, d.h. der Aufteilung eines Marktes unter wenigen Unternehmen – so Dix 2013: 36. Zu diesem Problem auch Vesting 2012: 23.

entscheidet über den Zugang zu bestimmten Einrichtungen. Vor allem ist es ohne weiteres möglich, dass private und öffentliche Stellen sich gegenseitig mit Informationen versorgen, die diese dann für ihre je eigenen Zwecke einsetzen.

6 Die offene Flanke : Europäisierung und „Globalisierung"

Digitale Identifizierung und ihr Recht sind längst keine allein nationalen Aufgaben mehr. Grenzüberschreitender Handel, Verkehr und Kriminalität – um nur einige Beispiele zu nennen – haben längst zwischenstaatliche und supranationale Rechtssetzungsaktivitäten ausgelöst. Dabei dürften die von der EU-Kommission (KOM (2010) 385 endg., zu Eurodac) genannten Grundsätze und Grundlagen einer europaweiten Identifizierungsinfrastruktur auch über ihren Anlass hinaus Allgemeingut werden: *Dezentrale Struktur; Zweckbindung; limitierte Parallelstrukturen und Funktionsüberschneidungen; limitierte und kontrollierte Zugriffsrechte; Variable Regeln für die Datenspeicherung und -verarbeitung; wirksames Identitätsmanagement* einschließlich der verstärkten, aber zugleich noch auszugestaltenden Nutzung biometrischer Daten*; Datensicherheit durch EU-Lösungen; Notwendigkeit und Differenzierung von Überprüfungsmechanismen.* Dazu dürften verstärkte Bemühungen um Netzsicherheit gegen Ausspähung durch Dritte aus dem In- und Ausland, sowie Begrenzungen jedenfalls einzelner Geheimdienstaktivitäten zählen. Doch steckt gerade hier der Teufel nicht selten im Detail: Sie bedürfen weiterer Abstimmung und Harmonisierung mit den Bemühungen um eine Vereinheitlichung des europäischen Datenschutzrechts. Auch lässt eine sich anscheinend verdichtende Grundrechtsprechung des EuGH erneut die Frage nach dem Niveau europäischen Datenschutzes aufkommen. Digitale Identifizierung ist also nicht mehr Aufgabe des nationalen Rechts und der nationalen Juristen allein. Und sie steht in einem sich noch weiter ausdifferenzierenden rechtlichen Kontext im Mehrebenensystem. Es gibt also noch viel zu tun!

Literatur

Albrecht, Astrid (2003): *Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz*, Baden-Baden: Nomos.

Bizer, Johann (2003): „Das Recht auf Anonymität in der Zange gesetzlicher Identifizierungspflichten“, in: Bäumler Helmut und von Mutius Albert, *Anonymität im Internet – Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts*, Braunschweig/Wiesbaden: Vieweg, 78-94.

Böckenförde, Ernst-Wolfgang (1976): „Die Bedeutung der Unterscheidung von Staat und Gesellschaft im demokratischen Sozialstaat der Gegenwart (1972)“, in: ders. (Hrsg.), *Staat und Gesellschaft*, Darmstadt: Wissenschaftliche Buchgesellschaft, 395-431.

Bösing, Sebastian (2005): *Authentifizierung und Autorisierung im elektronischen Rechtsverkehr*, Baden-Baden: Nomos.

Britz, Gabriele (2007): *Freie Entfaltung durch Selbstdarstellung. Eine Rekonstruktion des allgemeinen Persönlichkeitsrechts aus Art. 2 I GG*, Tübingen: Mohr Siebeck.

Britz, Gabriele (2012): „Elektronische Verwaltung“, in: Hoffmann-Riem Wolfgang, Schmidt-Aßmann Eberhard und Voßkuhle Andreas (Hrsg.), *Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen*, 2. Auflage, München: C.H. Beck, 435–492.

Bull, Hans Peter (2011): *Informationelle Selbstbestimmung – Vision oder Illusion? Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit*, 2. Auflage, Tübingen: Mohr Siebeck.

Burkart, Roland (2002): *Kommunikationswissenschaft*, 4. Auflage, Stuttgart: UTB.

Di Fabio, Udo (2011): „Kommentierung des Art. 2 Abs. 1 GG“, in: Maunz, Theodor und Dürig, Günter (Hrsg.), *Grundgesetz-Kommentar*, München: C.H. Beck.

Dammann, Ilmer (2011): *Der „Kernbereich privater Lebensgestaltung“,* Berlin: Duncker & Humblot.

Dix, Alexander (2013): „Thesen zum Referat beim 69. Deutschen Juristentag München (2012), Abteilung IT- und Kommunikationsrecht, Persönlichkeits- und Datenschutz im Internet – Anforderungen und Grenzen einer Regulierung“, in: *Verhandlungen des 69. Deutschen Juristentages - München 2012 Band II/1: Sitzungsberichte - Referate und Beschlüsse*, München: C.H. Beck, 35-40.

Dreier, Horst (1987): „Erkennungsdienstliche Maßnahmen im Spannungsfeld von Gefahrenabwehr und Strafverfolgung“, in: *Juristenzeitung*, 1009-1017.

Dreier, Horst (2013): „Kommentierung des Art. 2 Abs. 1 GG“, in: ders. (Hrsg.), *Grundgesetz-Kommentar, Band 1 (Art. 1-19)*, 3. Auflage, Tübingen: Mohr Siebeck.

Druey, Jean Nicolas (1995): *Information als Gegenstand des Rechts*, Zürich: Schulthess Verlag.

Eickelpasch Rolf und Rademacher Claudia (2004): *Identität*, Bielefeld: Transcript Verlag.

Ellenberger, Jürgen (2014): „Kommentierung des § 125 BGB“, in: Palandt, Otto (Begr.), *Kommentar zum Bürgerlichen Gesetzbuch (BGB)*, 73. Auflage, München: C.H. Beck.

Gerhards, Julia (2010): *(Grund-) Recht auf Verschlüsselung?,* Baden-Baden: Nomos.

Gusy, Christoph (1983): „Grundrechtsschutz vor staatlichen Informationseingriffen“, in: *Verwaltungsarchiv* (74), 91-111.

Gusy, Christoph (2003): „Grundrechtsschutz des Privatlebens“, in: Zehetner, Franz (Hrsg.), *Festschrift für Hans-Ernst Folz*, Wien u.a.: Neuer Wissenschaftlicher Verlag, 103-115.

Gusy, Christoph (2012): „Polizeiliche Datenverarbeitung zur Gefahrenabwehr“, in: *Zeitschrift für das Juristische Studium*, 155-167.

Gusy, Christoph (2014): *Polizei- und Ordnungsrecht*, 9. Auflage, Tübingen: Mohr Siebeck.

Heller, Christian (2011): *Post-Privacy. Prima leben ohne Privatsphäre*, München: Beck.

Hobert, Guido (1998): *Datenschutz und Datensicherheit im Internet. Interdependenz und Korrelation von rechtlichen Grundlagen und technischen Möglichkeiten*, Frankfurt: Peter Lang.

Hoeren, Thomas (Hrsg.) (2014): *Big Data und Recht*, München: C.H. Beck.

Hornung, Gerrit (2005): *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, Job Card-Verfahren*, Baden-Baden: Nomos.

Hornung, Gerrit und Möller, Jan (2011): *Kommentar zum Passgesetz und Personalausweisgesetz*, München: C.H. Beck.

Hornung, Gerrit und Hofmann, Kai (2013): „Ein ‚Recht auf Vergessenwerden‘? Anspruch und Wirklichkeit eines neuen Datenschutzrechts“, in: *Juristenzeitung*, 163-170.

Kleih, Björn-Christian (2010): *Die strafprozessuale Überwachung der Telekommunikation – unter besonderer Berücksichtigung drahtloser Netzwerke*, Baden-Baden: Nomos.

Kloepfer, Michael (2002): *Informationsrecht,* München: C.H. Beck.

Mayer-Schönberger, Viktor (2011): *Delete. Die Tugend des Vergessens in digitalen Zeiten*, 2. Auflage, Berlin: Berlin University Press.

Meier, Andreas (2007): *Relationale und postrelationale Datenbanken*, 6. Auflage, Heidelberg: Springer.

Oermann, Markus und Staben, Julian (2013): „Mittelbare Grundrechtseingriffe durch Abschreckung? Zur grundrechtlichen Bewertung polizeilicher ‚Online-Streifen‘ und ‚Online-Ermittlungen‘ in sozialen Netzwerken“, in: *Der Staat* 52(4), 630-661.

Rawls, John (1979): *Eine Theorie der Gerechtigkeit*, Frankfurt am Main: Suhrkamp Verlag.

Schaar, Peter (2014): *Überwachung total. Wie wir in Zukunft unsere Daten schützen*, Berlin: Aufbau Verlag.

Schild, Hans-Hermann (2013): „Kommentierung von § 3 BDSG“, in: Wolff, Heinrich-Amadeus und Brink, Stefan (Hrsg.), *Datenschutzrecht in Bund und Ländern – Grundlagen, bereichsspezifischer Datenschutz, BDSG*, München: C.H. Beck.

Sievers, Malte (2003): *Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes*, Baden-Baden: Nomos.

Spindler, Gerald (2012): *Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung. Gutachten F zum 69. Deutschen Juristentag*, München: C.H. Beck.

Strandburg, Katherine J. (2014): „Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Context", in: Lane Julia, Stodden Victoria, Bender Stefan und Nissenbaum Helen (Hrsg.), *Privacy, Big Data and the Public Good*, New York: Cambridge University Press, 5-43.

Vesting, Thomas (2012): „Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung", in: Hoffmann-Riem Wolfgang, Schmidt-Aßmann Eberhard und Voßkuhle Andreas (Hrsg.), *Grundlagen des Verwaltungsrechts, Band II: Informationsordnung, Verwaltungsverfahren, Handlungsformen*, 2. Auflage, München: C.H. Beck, 1-34.

Watzlawick Paul, Beavin Janet Helmick und Jackson John D. (2011): *Menschliche Kommunikation. Formen, Störungen, Paradoxien*, 12. Auflage, Bern: Hans Huber Verlag.

Weidner-Braun, Ruth (2012): *Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im WWW nach deutschem öffentlichen Recht*, Berlin: Duncker & Humblot.

Worms, Christoph und Gusy, Christoph (2012): „Verfassung und Datenschutz. Das Private und das Öffentliche in der Rechtsordnung", in: *Datenschutz und Datensicherheit*, 92-99.

Technische Voraussetzungen elektronischer Identifikation

Lexi Pimenidis

Der Inhalt dieses Kapitels ist es darzulegen, welche technischen Voraussetzungen für elektronische Identifikation und Identitäten notwendig sind.

Hierzu gehen wir als erstes auf notwendige informationstechnische Grundlagen ein. Im weiteren Verlauf verwenden wir dieses Wissen, um informationstechnisch zu analysieren, welche Möglichkeiten gegeben sind, Personen und Identitäten in Computersystemen zu erkennen oder zu verknüpfen. Komplementär hierzu diskutieren wir daraufhin, mittels welcher Technologien sich Individuen oder Gruppen diesen Möglichkeiten, gegebenenfalls mit Absicht, widersetzen können.

Die beiden letzten Abschnitte widmen sich der Frage, wie die stetig wachsenden Kapazitäten moderner IT-Systeme Einfluss auf unsere Teilhabe an modernen Technologien nehmen. Dies erfolgt sowohl unter dem Aspekt der möglichen Datenspeicherung als auch im Licht des 2013 durch Edward Snowden bekannt gemachten realen Ausmaßes geheimdienstlicher Spionage.

1 Begriffe und Terminologie

Im Kontext elektronischer Identitäten gibt es mehrere technische Begriffe, die in der Forschung international einheitlich verwendet werden.[1]

- Anonym
  Ein Nutzer ist innerhalb eines gegebenen Systems anonym gegenüber einem Beobachter, solange ihn dieser mit den ihm zur Verfügung stehenden Mitteln nicht von den anderen Nutzern unterscheiden kann. Insbesondere ist man gegenüber einem Beobachter anonym, wenn die-

1 Eine detailliertere Besprechung dieser und weiterer Begriffe sind dem Online-Dokument “A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version v 0.34, 10. Aug 2010) ” (Pfitzmann und Hansen 2010) zu entnehmen.

ser mehrere Einzelaktionen eines Nutzers nicht miteinander in Verbindung bringen („verketten“) kann.
Ein modernes Beispiel anonymer Nutzung ist das Surfen auf einer Webseite. Hierbei ist ein Nutzer dem Betreiber der Webseite gegenüber anonym, solange er keine persönlichen Daten preisgibt und der Betreiber nicht über Zusatzwissen verfügt, um den Nutzer zum Beispiel über die verwendete IP-Adresse oder Cookies zu identifizieren. Kehrt der gleiche Nutzer an einem anderen Tag mit einer anderen IP-Adresse wieder, so kann man den zweiten Besuch nicht ohne weiteres mit dem ersten in Verbindung bringen. Diese Anonymität gilt jedoch nicht gegenüber einem lokalen Netzwerkadministrator des Nutzers, der den Besuch protokolliert haben könnte.

- Pseudonym
  Im Gegenzug zur Anonymität kann ein Beobachter Aktionen eines pseudonymen Nutzers miteinander verbinden. Ähnlich wie bei anonymem Handeln kann er diese Beobachtungen jedoch weiterhin nicht mit einer realen Person in Verbindung bringen.
  Ein klassisches Pseudonym sind E-Mailadressen, die keine oder nur sehr allgemeine persönliche Informationen enthalten – die Pseudonymität ist dann gegenüber anderen E-Mailnutzern gewahrt, nicht jedoch gegenüber Angestellten des E-Mailproviders, wenn bei der Vergabe der E-Mailadresse die Identität des Nutzers offenbart wurde.

- Identifizierte Person
  Ist eine Handlung oder ein digitaler Datensatz eindeutig einer realen Person zuzuordnen, so ist dieser weder anonym noch pseudonym. Die Person ist identifiziert.

Wichtig zu merken ist, dass ein Zustand möglicher Anonymität oder Pseudonymität immer nur gegenüber einer bestimmten Menge von Menschen erreicht werden kann. Typische Klassen von Menschen, gegen die man seine persönlichen Daten schützen will sind (Panchenko und Pimenidis 2006):

- Dritte Parteien, als Personen, die weder mit einem selbst, noch mit dem Kommunikationspartner zu tun haben, noch mit der Kommunikation dazwischen. Beispiele hierfür sind für die meisten Personen in Europa die chinesische Regierung oder ein US-amerikanischer Geheimdienst.

- Der Kommunikationspartner ist möglicherweise ebenfalls eine Person, gegenüber der gewisser Datenschutzansprüche bestehen. Dies gilt zum Beispiel für Webseitenbetreiber.
- Die lokalen Infrastrukturanbieter, wie zum Beispiel Telekommunikationsunternehmen oder Netzwerkadministratoren, haben weitreichende Möglichkeiten, sich über die jeweiligen Nutzer und Kunden zu informieren. Die meisten dieser Möglichkeiten sind illegal, ihr Einsatz ist in der Regel jedoch weder zu erkennen noch nachzuweisen.
- Polizeibehörden und Geheimdienste haben in rechtsstaatlichen Nationen ein legitimes Interesse und den Auftrag, die Identität bestimmter Personen unter rechtlich näher umschriebenen Voraussetzungen aufzudecken. In Diktaturen hingegen sind sie annähernd allwissende Entitäten, die ohne solche rechtsstaatlichen Beschränkungen operieren.

Ein wichtiger Teil jeder Analyse im Datenschutz ist es folglich zu bestimmen, gegen welche natürlichen und juristischen Personen Ansprüche auf Datenschutz bestehen und wie diese durchzusetzen sind. Dieser Vorgang wird als Teil vieler Sicherheitsprozesse auch „Risikoanalyse“ genannt.

2 Informationstechnische Grundlagen

Informationstechnische Verfahren werden bei der Verwaltung von elektronischen Identitäten benutzt, um mit Sicherheit Aussagen treffen zu können. Typische Fragestellungen hierbei sind:

- Welche reale Person ist der Nutzer?
- Welche der gespeicherten Identitäten entspricht dem Nutzer?
- Was darf der Nutzer?

In den folgenden drei Kapiteln werden wir die Grundlagen der Beantwortung dieser Fragen eingehend erläutern.

2.1 Die Identifizierung

Zuerst beantworten wir die Frage „Welche reale Person ist der Nutzer?“. Dieses ist häufig die erste und initiale Frage im Rahmen der Nutzung eines IT-Systems. Hierbei wird versucht zu bestimmen, welche reale Person der Nutzer ist. Die Exaktheit, mit der dies bestimmt wird, hängt von unterschiedlichen Faktoren ab, wie

- der Gesetzeslage: so sind zum Beispiel Anbieter von E-Maildiensten oder nicht jugendfreien Angeboten in Deutschland und vielen anderen Ländern gesetzlich verpflichtet, die Identität des Nutzers zweifelsfrei festzustellen,
- der Art des Services: spielt für es für den Betreiber des Services keine Rolle zu wissen, welchen Namen der Nutzer hat, so gibt es keinen Bedarf, diesen zu erheben,
- technischen und sonstigen Restriktionen: die Verlässlichkeit der Eingabe fast aller Merkmale des Nutzers (Name, Alter, biometrische Merkmale, Geschlecht und weitere) lässt sich insbesondere in Online-Anwendungen nur im Ausnahmefall zuverlässig bestätigen.

Dieser Vorgang wird auch als „Identifizierung“ bezeichnet und verbirgt sich hinter der „Registrierung“-Funktionalität eines Dienstes. Im Rahmen der Beantwortung der Frage nach der realen Person wird dem Nutzer in der Regel ein internes Kennzeichen zugewiesen, um den erfolgreichen Vorgang technisch zu dokumentieren (Login, Benutzername).

2.2 Die Authentifizierung

Bei der Frage „Welche der gespeicherten Identitäten entspricht dem Nutzer?“ geht es um die Beantwortung der Frage, ob ein Nutzer sich bereits bei einem Dienst erfolgreich identifiziert hat und wenn ja, welcher der internen Identitäten er entspricht.

Dieser Vorgang wird auch als „Authentifizierung“ bezeichnet und ist den meisten Nutzern auch als „Anmelde“-Funktion oder „Login“ bekannt. Notwendigerweise muss hier eine Datenbank mit mindestens einer gespeicherten Identität vorliegen.

Die einfachste und üblichste Möglichkeit, eine Authentifizierung durchzuführen ist es, den Nutzer selber zu bitten, sich zu identifizieren, indem er den ihm zugewiesenen Benutzernamen eingibt. Dies alleine ist allerdings missbrauchsanfällig, weil diese gegebenenfalls öffentliche Information von jeder beliebigen Person eingegeben worden sein könnte. Um dies zu verhindern, wird oft mindestens ein weiteres der folgenden drei Kriterien genutzt, um zu überprüfen, ob die Identität der eingebenden Person mit der vorgegebenen Identität des Benutzernamens übereinstimmt:

- Etwas, was die Person weiß.
  Hierbei wird üblicherweise ein Passwort abgefragt; aber auch die bekannten "Sicherheitsfragen" nach Grundschullehrern, dem ersten Auto etc. sind Informationen, die die Echtheit des Benutzernamens untermauern sollen.
- Etwas, was die Person hat.
  Hierbei ist an Chipkarten oder andere Token zu denken, wie den neuen Personalausweis, die elektronische Gesundheitskarte oder andere Chipkartenausweise. Wenn ein kompliziertes und sehr sicheres Passwort auf einen Zettel geschrieben wird, dann fällt jedoch auch der Zettel in diese Kategorie, da er ein physischer Gegenstand ist, ohne dessen Besitz das Passwort nicht eingegeben werden kann.
- Biometrische Merkmale der Person selbst.
  Ein Fingerabdruck, die Muster der Iris, die Größe, das Gewicht etc. sind Beispiele hierfür. Biometrische Merkmale sind aktuell immer noch nicht sicher genug, um als alleiniges Merkmal für eine Authentifizierung genutzt zu werden, da sie im Verlauf des Lebens einer Person Schwankungen unterliegen können und oft auch nicht ohne weiteres gegen Missbrauch und Kopieren gesichert werden können. Man denke an die Veröffentlichung des Fingerabdrucks des damaligen Innenministers Schäuble durch den CCC im Jahre 2008.

Für besonders sicherungsbedürftige Systeme wird eine Kombination mehrerer dieser Merkmale genutzt; üblich ist ein physischer Gegenstand und ein Passwort, wie bekannt aus den ChipTAN oder mTAN-Systemen der deutschen Banken.

Im Kontext der „Verkettung“ werden wir die Authentifizierung noch einmal wieder treffen: Es ist nämlich auch möglich, einen Nutzer ohne bewusste Aktivitäten seinerseits oder passive Hilfestellung anderer zu authentifizieren. Ein bekanntes Beispiel hierfür sind Werbe-Tracker, die mittels technischer Methoden wie Cookies mehrere Aktionen einer Person miteinander verkettbar machen. Daher spricht man hier in Abgrenzung zur „Authentifizierung“, die aktiv vom Nutzer gesteuert und erlebt wird, von einer „Verkettung“, die im Hintergrund durchgeführt wird.

Die gleichen drei Kriterien, die wir bei der legitimen Authentifizierung genutzt haben, können auch hier betrachtet werden:

- Die Abfrage von Wissen einer Person; dies kann auch unter Zuhilfenahme von rhetorischen Tricks und der Ausnutzung sozialer Prägung

schleichend erfolgen. Auf der einen Seite wird diese Technik oft von Hackern im Rahmen von Social Engineering Angriffen (Mitnick und Simon 2003) verwendet um so viele Informationen von einer Person zu erfahren, dass sie sich selbst später glaubhaft als diese Person ausgeben können.

Bekannt ist auch die offene Frage von Facebook „What's on your mind?“, die Menschen dazu verleiten kann, mehr von sich zu preiszugeben, als sie sinnvollerweise sollten.

- Logische Gegenstände werden von der Werbeindustrie im Internet genutzt, um Aktionen eines Nutzers zu verketten: Ohne das explizite Wissen der meisten Nutzer werden deren Browser mit Cookies „verwanzt“, die beim Abrufen von Webseiten mitgesendet werden und so eine weitreichende Analyse der Interessen ermöglichen. Die aufgrund rechtlicher Vorgaben inzwischen vielfach vorhandenen Hinweise ändern daran wenig, weil die allermeisten Nutzer nicht über das technische Wissen verfügen, um zu verstehen, was ein Cookie ist und was es genau tut.

  Das Tracking mittels physischer Gegenstände betrifft auch Handys und andere mobile Endgeräte, etwa im Rahmen von Funkzellenabfragen. Diese Technik wurde in der Presse prominent zum Beispiel für die Erfassung von Demonstrationsteilnehmern durch die Polizei in Dresden im Jahre 2011 thematisiert.
- Biometrische Merkmale finden bei Videoüberwachung weitreichende Verwendung, um Personen ohne deren aktive Mitarbeit zu authentifizieren.

Grundlegend ist zu wiederholen, dass eine Authentifizierung drei Dinge benötigt:

- eine Datenbank möglicher Identitäten,
- Daten, die ein Individuum beschreiben, sowie
- Algorithmen, die die Daten mit denen in der Datenbank abgleichen,

Die Qualität einer Authentifizierung hängt entscheidend von allen drei Faktoren ab. Je größer die Datenbank, je unspezifischer die Beschreibung eines Individuums oder je simpler der Algorithmus, der den Abgleich vornimmt, desto wahrscheinlicher ist es, dass eine Fehlentscheidung getroffen wird.

Nutzer können auch gegen ihren Willen authentifiziert werden, zum Beispiel von der Werbe-Industrie. Diese nutzt sogenannte „Big Data“-

Techniken, um möglichst große Datenbanken von Nutzern aufzubauen. Diese Techniken basieren darauf, dass Menschen weniger individuell sind, als im Allgemeinen erwartet wird. So gibt es statistische Zusammenhänge zwischen Vorlieben, Hobbys, Einkaufsverhalten und fast allen anderen Aspekten einer Identität. Durch diese Möglichkeit der Bildung von Clustern wird es technisch möglich, Voraussagen über die Zukunft oder noch unbekannte Aspekte einer Person zu treffen, die eine signifikante Eintrittswahrscheinlichkeit haben. Somit können mit Hilfe von Personen, die wenig Wert auf Datenschutz legen und über die in den Datenbanken viele Informationen zur Verfügung stehen, zum Beispiel auch Aussagen über Personen getroffen werden, über die nur wenig bekannt ist.

2.3 Die Autorisierung

Wenden wir uns nun der Frage zu „Was darf der Nutzer?“. Im Anschluss an eine „Authentifizierung“ findet in der Regel eine „Autorisierung“ statt. Hierbei wird die Frage beantwortet, welche Privilegien, Rechte, Pflichten, Erlaubnisse etc. ein Nutzer hat.

Im Bereich der elektronischen Identitäten sind hier aus technischer Sicht hauptsächlich Möglichkeiten interessant, die ohne eine vorherige Authentifizierung funktionieren. Wird der Nutzer vorher authentifiziert, so ist dem System die Identität des Nutzers bekannt und es werden alle Daten mit dem Benutzerkonto verknüpft, die zur Autorisierung benötigt werden.

Fehlt eine Authentifizierung, oder soll sie aus Gründen des Datenschutzes nicht durchgeführt werden, können „Zero-Knowledge-Beweise“ eingesetzt werden (Quisquater und Guillou 1990). Dies ist eine Klasse von Algorithmen, mit denen ein Nutzer beweisen kann, dass er zum Beispiel eine Zugangsberechtigung zu einem System hat, ohne sich dem IT-System gegenüber zu authentifizieren. Das bedeutet, dass man zum Beispiel mittels eine Zero-Knowledge-Beweises einem Verlag gegenüber beim Abruf eines Artikels beweisen kann, dass man ein gültiges Abonnement bezieht, aber nicht offenlegen muss, welcher der Abonnementen man ist.

Ein Zero-Knowledge-Beweis funktioniert auf der technischen Ebene so, dass das IT-System mehrere Herausforderungen an den Nutzer sendet und dieser mittels seiner Zugangsdaten beweisen kann, dass er die gestellten Probleme lösen kann. Hieraus ergibt sich auch ein offensichtlicher Nachteil von Zero-Knowledge-Beweisen gegenüber klassischen Verfahren zur Autorisierung: Durch ihre Interaktivität sind sie deutlich rechenintensiver,

dauern deshalb länger und sind somit nur begrenzt in normalen Systemen einsetzbar.[2]

Eine weitere Möglichkeit der Autorisierung ohne Authentifizierung sind „Anonyme Credentials“ (Camenisch und Lysyanskaya 2001). Diese ermöglichen Erweiterungen zu den oben beschriebenen Möglichkeiten. So kann zum Beispiel im Betrugsfall eine vorher bestimmte vertrauenswürdige Person die Anonymität des Nutzers aufheben, und es ist möglich, die Nutzung der Credentials auf ein bestimmtes Maß zu beschränken, so dass der Nutzer sich zum Beispiel nur 50-mal bei einer Webseite anmelden kann. Außerdem sind Anonyme Credentials von reduzierter technologischer Komplexität, so dass sie sogar in den Chips von Smart-Cards enthalten sein können (Bichsel et al. 2009).

Verwandt mit Autorisierung ist das „Accounting“, also das Nachhalten der Zuweisung von dynamischen Ressourcen zu einem Nutzer. An dieser Stelle möchte ich kurz auf die Möglichkeiten von „elektronischem Geld“ eingehen; insbesondere unter dem Aspekt, elektronische Währungen ohne eine zentrale Instanz zu betreiben, die den Geldfluss beaufsichtigt. Das zentrale auftretende Problem in dieser Situation ist das mögliche „Double Spending“: Da elektronische Daten ohne Verlust beliebig reproduzierbar sind, muss eine Möglichkeit gefunden werden, um Nutzer daran zu hindern, den ihnen zugewiesenen Betrag mehrfach auszugeben. Ansonsten wäre jeder in der Lage, Geld zu „drucken“, und die Währung wäre in kürzester Zeit entwertet. Erste Lösungsideen sind von Chaum schon 1983 beschrieben worden (Chaum 1983), setzten jedoch Banken als vertrauenswürdige Parteien voraus. Aktuell sehen wir bereits erste praktische Umsetzungen, vor allem die „BitCoins“ (Nakamoto 2008).

Das Problem des „Double Spending“ wird im BitCoin-Netzwerk gelöst, indem alle Transaktionen in der Öffentlichkeit stattfinden. Durch die Bezeugung vieler unbeteiligter Netzwerkteilnehmer wird festgehalten, dass ein bestimmter Betrag zwischen zwei Parteien einvernehmlich ausgetauscht wurde. Die Notwendigkeit von zentralen Instanzen wurde hierdurch aufgelöst und ersetzt durch Kontostände, die an digitale Identitäten geknüpft sind. Diese beinhalten zwar per se keine Informationen, mit denen ein Nutzer als Person zu erkennen wäre. Sie können jedoch zum Beispiel über E-Mailadressen realen Nutzern plausibel zugeordnet werden,

2 Anwendungen in der realen Welt beschränken sich aktuell auf Domänen von Experten, die im Umgang mit kryptographischen Protokollen geschult sind. Siehe z.B. https://en.wikipedia.org/wiki/Secure_Remote_Password_protocol.

falls bei der Erstellung eines Nutzerkontos nicht hinreichend Wert auf Aspekte des Datenschutzes gelegt worden ist (Biryukov et al. 2014).

Somit verbleiben technische Pseudonyme, mit denen der Kreislauf des Geldes verfolgt werden kann (Ron und Shamir 2013). In diesem Sinne gibt es aktuell keine Möglichkeit digital zu bezahlen, die datenschutzfreundlicher ist als Bargeld; es gibt jedoch durchaus Methoden, mit denen datenschutzfreundlicher bezahlt werden kann, als mittels einer normalen Banküberweisung.

3 Verschlüsselung von Daten und elektronische Signaturen

Im Rahmen von sicheren und datenschutzfreundlichen IT-Systemen wird überdies Gebrauch von diversen weiteren informationstechnische Verfahren gemacht. Besonders hervorzuheben ist hierbei die Verschlüsselung von Daten – sei es bei der Übertragung von einem System zu einem anderen, oder bei der Ablage auf einem persistenten Speichermedium, wie zum Beispiel einer Festplatte oder einem USB-Stick.

3.1 Verschlüsselungsverfahren

Die wichtigste Anmerkung im Bereich der Verschlüsselung ist, dass eine zweifelsfreie Authentifizierung, sei es einer Person oder eines Systems, notwendige Vorbedingung jeder sinnvollen Verschlüsselung ist. Fehlt diese, so ist es für eine dritte Partei oft ohne weiteres möglich, sich in die Kommunikation einzuklinken, Daten mitzulesen oder zu manipulieren. Dies liegt ganz offensichtlich an der Tatsache, dass für eine effektive Verschlüsselung im Allgemeinen ein Schlüssel[3] benötigt wird, welcher nur den beiden Kommunikationsteilnehmern bekannt sein darf (Kerckhoffs 1883). In der elektronischen Welt des Internets gibt es keine unmittelbare persönliche Kommunikation zwischen einem Nutzer und zum Beispiel einem Webshop, sondern nur einen technisch vermittelten Informations-

3 Umgangssprachlich und für klassische Formen der Verschlüsselung ist ein sogenanntes „Passwort“ der gemeinsame Schlüssel. Für einige moderne Verfahren spielen Passwörter immer noch eine Rolle, in der Regel wird der gemeinsame Schlüssel jedoch durch mathematische Verfahren aus teils öffentlichen und teils geheimen Informationen berechnet.

austausch, der gegebenenfalls das Gefühl einer direkten persönlichen Kommunikation vermitteln kann. Dieser ist nicht ohne Sicherheitsprobleme zum Austausch von vertraulichen Schlüsseln geeignet. Daher müssen aufwendige und fehleranfällige Verfahren benutzt werden. Die Komplexität des Problems, einen sicheren Schlüsselaustausch mit einer unbekannten Person durchzuführen, wird unter anderem dadurch untermauert, dass selbst *die* zentrale Sicherheitsbibliothek des Internets, *openssl*, dies in den letzten 20 Jahren nicht geschafft hat.

Erst wenn die Identität des Kommunikationspartners hinreichend genau für die Zwecke der Kommunikation bestimmt ist, ergibt es Sinn, sich Gedanken über das Schlüsselmanagement zu machen. Für die Identifizierung verwendet man heute im Online-Kontext asymmetrische Kryptographie. Hierzu generiert jeder Teilnehmer an einem informationstechnischen System einen „elektronischen Ausweis", der aus zwei Teilen besteht: einem privaten und einem öffentlichen Teil, die jeweils durch eine sehr große Zahl dargestellt werden können -- aktuell werden Zahlen mit mindestens 600 Dezimalstellen empfohlen (das entspricht 2048 Bit). Diese sind mathematisch so gestaltet, dass es zu jedem öffentlichen Teil nur genau einen privaten Teil geben kann und dass es nicht möglich ist, den privaten Teil aus dem öffentlichen zu berechnen. Diese Eigenschaften sind zum Beispiel bei Verwendung des RSA-Algorithmus[4] gegeben. Um sich mit dem öffentlichen Teil authentifizieren zu können, benötigt man eine Zuordnung von realen Identitäten zu diesen Zahlen, denn es handelt sich um eine Authentifizierung mittels einer Zahl.

Im Internet gibt es hierzu etwas mehr als 100 vertrauenswürdige Parteien („Zertifizierungsstellen"), bei denen ein Nutzer zu seinem elektronischen Ausweis seinen Namen und weitere persönliche Daten hinterlegen kann und zertifiziert wird, dass die persönlichen Daten zu dem vorgelegten öffentlichen Schlüssel gehören.[5] Weist man nun also den öffentlichen Teil des elektronischen Ausweises zusammen mit dem ausgestellten Zertifikat vor, gibt es mathematische Verifikationsalgorithmen, mit denen jedermann feststellen kann, ob das Zertifikat zu dem öffentlichen Teil des Schlüssels passt, ob die Person im Besitz des geheimen Teil des Schlüssels

---

4 http://de.wikipedia.org/wiki/RSA-Kryptosystem.

5 Diese Prozesse sind nicht staatlich reguliert und folglich rechtlich nicht geregelt. Die Qualität der Zertifizierungsprüfung und damit der Authentifizierung kann variieren (anders als bei regulierten Systemen wie der qualifizierten elektronischen Signatur).

ist, ohne ihn zeigen zu müssen, und ob das Zertifikat zu der Stelle passt, mit der man eigentlich kommunizieren wollte.

Erst jetzt ist man in einer Situation, um sinnvoll Schlüsselmanagement betreiben zu können und daraufhin die Daten verschlüsselt auszutauschen. Für jede Art der sinnvollen Verschlüsselung wird zwischen den Teilnehmern ein gemeinsamer geheimer Code vorausgesetzt (Kerckhoffs 1883).

Moderne Verfahren benutzen den Kontext der Authentifizierung, um durch mathematische Verfahren ein gemeinsames „Codewort" zwischen den Kommunikationsteilnehmern zu berechnen (in Computersystemen ist dieses „Codewort" eine sehr lange Zahl). Mit dem Verfahren von Diffie und Hellman (1976) ist es zwei Parteien möglich, sich auf ein Codewort zu einigen, ohne dass dieses „ausgesprochen", das heißt übermittelt werden muss. Das einmal berechnete Codewort kann mehrfach verwendet werden, sollte jedoch in regelmäßigen Intervallen durch ein neues ersetzt werden. Die Dauer der Benutzung hängt davon ab, wie stark man das Interesse von Dritten beurteilt, vom Inhalt der Kommunikation Kenntnis zu nehmen, sowie von der Güte der verwendeten Verschlüsselungsverfahren.

Haben zwei Parteien einen gemeinsamen geheimen Code berechnet, können im Folgenden Daten verschlüsselt werden. Hiermit kann der Empfänger der Daten nicht nur sicherstellen, dass die Kommunikation vertraulich war, sondern auch, dass kein Dritter die Daten manipuliert oder einzelne Teile der Daten unterschlagen hat. Hierzu werden die Daten mit Hilfe des öffentlichen Teils des Schlüssels und des gemeinsamen geheimen Codes so umgerechnet, dass nur der Besitzer des geheimen Teils des Schlüssels diese Daten wieder in ihre unverschlüsselte Form überführen kann.

Für eine detailliertere Erläuterung der technischen Details gibt es eine Fülle an Literatur, die jedes Wissensniveau und Interesse abdeckt. Deshalb wird hier auf eine weitere Einführung verzichtet. Eine kurze Auswahl passender Literatur beinhaltet (Schneier 1996) und (Anderson 2008).

3.2 Die elektronische Signatur

Zertifizierungsstellen, welche als Basis für die Verschlüsselung beschrieben wurden, können auch für elektronische Signaturen genutzt werden. Hierzu bedient man sich der Tatsache, dass es eine mathematische Verkettung zwischen einer realen Identität und einem öffentlichen Teil eines Schlüssels gibt. Anders als bei der Verschlüsselung, bei der man mit dem

öffentlichem Teil des Schlüssels Daten so kodiert, dass sie nur ein spezifischer Empfänger entschlüsseln kann, funktioniert die elektronische Signatur genau entgegengesetzt: Der Besitzer des geheimen Schlüssels berechnet zu einem Dokument eine Zahl, welche die Signatur darstellt. Die Korrektheit und Zugehörigkeit zu dem zu unterschreibenden Dokument kann jedermann mit Hilfe des öffentlichen Schlüssels verifizieren. Es ist jedoch technisch weitestgehend ausgeschlossen, dass diese Zahl von einer Person berechnet worden sein kann, die nicht im Besitz des geheimen Teils des Schlüssels gewesen ist.

Hiermit haben wir die kurze Einführung in technische Aspekte abgeschlossen und werden uns jetzt der Bedeutung dessen zuwenden, was sich aus der Anwendung dieser Grundlagen in modernen IT-Systemen ergibt.

4 Technische Möglichkeiten der Wiedererkennung

In den folgenden Abschnitten wollen wir uns mit der Bedeutung technischer Wiedererkennungsmöglichkeiten für den einzelnen Nutzer auseinandersetzen.

4.1 Verkettung

In der Praxis ist es oft weniger von Interesse, welche Identität jemand hat, sondern vielmehr, ob die Person bestimmte Eigenschaften besitzt. Diese können weitestgehend alltäglich (War dieser Nutzer schon einmal da? Ist er an einem bestimmten Produkt interessiert?), auf Finanzen bezogen (Wie hoch ist das Risiko, dass diese Person einen Kredit nicht zurückzahlen kann?) oder sehr persönlich sein (Wer ist ein möglicher Sexualpartner für diese Person?). Weiterhin reicht es oft aus, diese Eigenschaft mit einer bestimmten Wahrscheinlichkeit treffen zu können, wie zum Beispiel 80% oder 99%.

Häufig reichen bereits geringe Informationsschnipsel aus, um auf erstaunlich hohe Aussagewahrscheinlichkeiten zu kommen. Das einfachste Beispiel ist die Fähigkeit eines Webbrowsers, Cookies zu speichern. Hiermit können spezialisierte Servicebetreiber, wie zum Beispiel Google, nachverfolgen, zu welcher Uhrzeit eine Person auf welcher Webseite surft, ob sie im Büro, zu Hause oder mit dem Handy unterwegs ist, und zumindest auch grob, welche Aktionen sie auf dieser Webseite durchführt. Über

die Auswahl der regelmäßig besuchten Nachrichtenportale lässt sich bereits eine zuverlässige Aussage treffen, welche politische Gesinnung eine Person hat und durch die Nachrichtenauswahl, wie politisch aktiv sie ist. Im Fall von Suchmaschinen kommt oft dazu, dass alle Suchanfragen, die je über Google getätigt werden, im gleichen Profil gespeichert werden. Besonders pikant ist, dass Suchmaschinen heute oft genutzt werden, um den Besuch bei einem Arzt, Rechtsanwalt oder vergleichbarem Fachexperten vorzubereiten oder zu ergänzen und deshalb Fragen zum Umgang mit prekären Situationen dort eingegeben werden. So entsteht mit der Zeit ein Archiv aus Informationen, das mehr oder weniger alle Lebensbereiche des Nutzers abbildet.

Die nächste Ebene der Analyse basiert auf der Tatsache, dass Menschen im Allgemeinen deutlich weniger individuell sind, als sie denken. So gibt es zwischen einzelnen Eigenschaften oft starke Zusammenhangswahrscheinlichkeiten: Hat ein Mensch Kinder und ein Eigenheim, so ist die Wahrscheinlichkeit hoch, dass er auch Haustiere besitzt. Hat ein Dienstanbieter die oben beschriebenen Datenmengen (also quasi eine Lebensbeschreibung von vielen Millionen Menschen) gesammelt, ist es trivial solche Zusammenhänge statistisch zu erkennen – aber vor allem: diese in einem beliebigen Zusammenhang zu verknüpfen. So kann aus einem Profil bei Facebook mit 78-Prozentiger Wahrscheinlichkeit die sexuelle Orientierung einer Person vorhergesagt werden, selbst wenn es keine direkte Information zu diesem Themenbereich enthält (Jernigan und Mistree 2009). Es sind auch Fälle bekannt geworden, wo Nutzern teurere Angebote unterbreitet worden sind, weil sie mit einem Mac-Computer nach Produkten gesucht haben (Mattioli 2012). Das Verfolgen der Nutzer passiert nicht nur im Internet, sondern auch außerhalb; so können Mobiltelefone von jeder Technik-affinen Person wiedererkannt werden (Datoo 2013).

Möglich macht dies die Formel von Bayes.[6] Verfügt man über eine Tabelle, die darüber Auskunft gibt, mit welcher Wahrscheinlichkeit die Zielgruppe eine bestimmte Handymarke präferiert, sich in bestimmten Stadtteilen aufhält oder wie oft sie die Bahn benutzt, so kann man rückwärtsgerichtet aus der Tatsache, ob jemand die Bahn benutzt, bereits eine erste Aussage über andere Eigenschaften treffen.

Das Ausmaß dieser Möglichkeiten wird deutlich, wenn man sich vergegenwärtigt, dass digital gespeicherte Daten durch die immer stärker wer-

6 http://de.wikipedia.org/wiki/Satz_von_Bayes.

denden IT-Systeme *niemals* gelöscht werden müssen. Und was im Mittelalter noch das Sündenregister im Himmel war, ist heute die Datenbank im Internet, wo alle unsere Fehltritte für immer vorliegen werden und nicht nur zur Analyse von uns selbst, sondern auch für die Durchleuchtung Dritter herangezogen werden.

4.2 Staatlicher Bereich

Wie wir im Bereich Terminologie niedergelegt haben, sind die technischen Möglichkeiten staatlicher Stellen, sei es Polizei, Geheimdienste, Zoll, Steuerfahndung oder weiterer Stellen, besonders stark. Dies resultiert weniger aus tatsächlichem technischem Vermögen, sondern aus gesetzlichen Befugnissen, mittels derer ein Zugang zu sonst geschützten Daten erzwungen werden kann.

Anders als die Wirtschaft, welche sich mit Daten zufrieden geben muss, die der Nutzer über sich selber preisgibt (oft aus Unkenntnis über technische Hintergründe (Cookies) oder in Verkennung der Situation, wer die Daten lesen und auswerten kann), können staatliche Stellen auf Daten unserer Kernlebensbereiche Zugriff nehmen. Ein wichtiger Bereich hierbei sind Finanztransaktionen. In unserer Gesellschaft sind wir zu Spezialisten herangewachsen, die auf die Tätigkeiten anderer Personen angewiesen sind, und bezahlen deren Aufgaben immer öfter elektronisch. Der Anteil des elektronischen Geldtransfers lag dabei 2009 schon bei ca. 20%,[7] mit wachsender Tendenz.

Seit 2015 wird dieses Portfolio an Daten in Deutschland – erneut – durch die sogenannte Vorratsdatenspeicherung, also eine anlasslose Speicherung der meisten Kommunikations-Metadaten für mehrere Monate, ergänzt. Die Meta-Daten beinhalten hier insbesondere mindestens, wer wann mit wem kommuniziert hat, sowie die Position der Kommunikationsteilnehmer, sofern Mobiltelefone eingesetzt wurden. Bereits durch eine einfache Auswertung von Häufigkeiten kann hierbei festgestellte werden, in welchem Verhältnis sich zwei Personen zueinander befinden und ob dieses beruflicher oder privater Natur ist. Neben einem Bewegungsprofil aller Personen mit Mobiltelefonen kann man auch feststellen, wer sich mit wem wann und wo physisch getroffen hat.

---

7 S. http://www.einzelhandel.de/pb/site/hde/node/1061456/Lde/index.html.

Auf der technischen Seite sind die Speicherkapazitäten privater Anbieter und staatlicher Dienste mehr als enorm. Von Google ist bekannt, dass dort im Jahr 2010 täglich 20 Petabyte, also 20.000 Terabyte an Daten verarbeitet wurden. Wie 2013 bekannt wurde, betreibt die NSA in Utah ein Rechenzentrum mit der geschätzten Kapazität von mehreren Milliarden Terabyte,[8] so dass sie genug Speicherkapazität hat, um für jeden Menschen auf der Welt Daten von ca. einem Terabyte abzuspeichern und abrufbar zu machen. Zum Vergleich: 1 Terabyte entspricht einer aktuellen handelsüblichen Festplatte – die Menge an persönlichen digitalen Daten, die eine Person im Laufe ihres Lebens produzieren kann, liegt jedoch bei ca. der Hälfte dieser Größe.

5 Verhinderung von Identifikation, Verkettung und Tracking

Um eine Verkettung wirkungsvoll verhindern zu können, muss ein Nutzer vollständige Kontrolle über die Informationen ausüben, die im Rahmen einer Kommunikation ausgetauscht werden. Wichtig ist außerdem, dass der Nutzer bewusst entscheidet, welchen Entitäten gegenüber er einen bestimmten Schutzgrad wünscht.

In Abhängigkeit der benötigten OSI-Layer[9] gibt die folgende Tabelle Beispiele für mögliche Verkettungsmerkmale und Schutzmaßnahmen:

Ebene der Kommunikation	**Verkettungsmerkmal**	**Schutzmaßnahme**
Anwendungsebene	vom Nutzer eingegebene Daten	bewusste Eingabe von Falschinformationen, Weglassen von Informationen
Darstellungsebene	verwendeter Browser	Verwendung eines weitverbreiteten Browsers, Fälschung der Browserkennung
Sitzungsebene	Cookies im Browser	Löschen von Cookies nach jeder Nutzung
Transport- und Vermittlungsebene	IP-Adresse des Nutzers	Verwendung von Proxys oder Anonymisierungssoftware

8 S. http://de.wikipedia.org/w/index.php?title=Utah_Data_Center&oldid=127873204.
9 S. http://de.wikipedia.org/wiki/OSI-Modell.

Ebene der Kommunikation	Verkettungsmerkmal	Schutzmaßnahme
Sicherungsebene	MAC-Adressen der verwendeten Geräte	Wechsel der MAC-Adresse innerhalb der öffentlichen Bereiche
Bitübertragungsebene	Verwendete Chips in den Geräten	Kauf und Nutzung unterschiedlicher Geräte

Entscheidend für die Effektivität der Bemühungen um den Datenschutz ist dabei aber vor allem der bewusste Umgang mit den Informationen, auf die Einfluss genommen werden kann.

Dies bedeutet im besten Fall, dass sich ein Nutzer vor einer Aktion bewusst ist, welche Daten erzeugt werden, welche Personen diese möglicherweise zu sehen bekommen, was sie gegebenenfalls über ihn aussagen, welche Aussagekraft sie in Verbindung mit früheren Daten oder zukünftigen Daten haben und wie lange sie gespeichert werden können. Da dieses Bewusstsein jedoch auf die meisten Nutzer nicht zutrifft (weil sie entweder nicht über die erforderlichen analytischen oder technischen Fähigkeiten verfügen oder den Aufwand scheuen), wäre es wünschenswert, wenn technische Hilfestellungen den Nutzer unterstützen könnten, um Datensparsamkeit zu betreiben – vergleichbar einem Virenscanner, der für einen Nutzer bösartige von gutartiger Software unterscheidet.

In der Praxis sind Systeme, die sinnvollen Datenschutz erzeugen, bisher noch mit starken Einschnitten in die Benutzbarkeit verbunden (eine stark erhöhte Ladezeit von Webseiten ist hier das am ehesten wahrgenommene Phänomen), so dass die Verwendung dieser Programme selbst wohlwollenden Expertennutzern einiges an Willenskraft abverlangt. Technische Systeme, die auch für den Massenmarkt Datenschutz umsetzen, sind deshalb ein wichtiges und dringendes Forschungsthema. In der Praxis ist dagegen bisher der Verzicht auf die Teilnahme an modernen Medien oft leider die einzige praktische Methode, um die Privatsphäre zu schützen.

Literatur

Anderson, Ross (2008): *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed., Indianapolis: Wiley, online version: https://www.cl.cam.ac.uk/~rja14/book.html.

Bichsel Patrik, Camenisch Jan, Groß Thomas and *Shoup Victor* (2009): "Anonymous credentials on a standard java card", in: *CCS '09. Proceedings of the 16th ACM conference on Computer and communications security*, New York: ACM, 600-610.

Biryukov Alex, Khovratovich Dmitry, and *Pustogarov Ivan* (2014): "Deanonymisation of clients in Bitcoin P2P network", in: *CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, Ney York: ACM, 15-29.

Camenisch, Jan and *Lysyanskaya, Anna* (2001): "An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation", in: Pfitzmann, Birgit (Ed.), *Advances in Cryptology – EUROCRYPT 2001*, Lecture Notes in Computer Science 2045, 93-118.

Chaum, David (1983): "Blind signatures for untraceable payments", in: Chaum David, Rivest Ronald L. and Sherman, Alan T. (Eds.), *Advances in Cryptology. Proceedings of Crypto 82* (3), New York: Springer, 199-203.

Datoo, Siraj (2013): *This recycling bin is following you*, http://qz.com/112873/this-recycling-bin-is-following-you/.

Diffie, Whitfield and *Hellman, Martin E.* (1976): „New Directions in Cryptography", in: *IEEE Transactions on Information Theory* 22 (6), 644-654.

Jernigan, Carter und *Mistree, Behram F.T.* (2009): "Gaydar: Facebook friendships expose sexual orientation", in: *First Monday* 14(10), http://firstmonday.org/ojs/index.php/fm/article/view/2611/2302.

Kerckhoffs, Auguste (1983): "La Cryptographie Militaire", in: *Journal des sciences militaires* 9, 5-38 und 161-191.

Mattioli, Dana (2012): On Orbitz, Mac Users Steered to Pricier Hotels, in: *The Wall Street Journal*, 23 August 2012, http://www.wsj.com/articles/SB10001424052702304458604577488822667325882.

Mitnick, Kevin D. und *Simon, William* (2003): *Die Kunst der Täuschung: Risikofaktor Mensch*, Bonn: mitp-Verlag.

Nakamoto, Satoshi (2008): *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

Quisquater, Jean-Jacques and *Guillou, Louis* (1990): "How to explain zero-knowledge protocols to your children", in: Brassard, Gilles (Ed.), *Advances in Cryptology - CRYPTO '89*, Lecture Notes in Computer Science 435, 628-631.

Panchenko, Andriy and *Pimenidis, Lexi* (2006): "Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication", in: Leitold, Herbert and Markatos, Evangelos P. (Eds.): *Communications and Multimedia Security. 10th IFIP TC-6 TC-11 International Conference, CMS 2006, Heraklion, Crete, Greece, October 19-21, 2006. Proceedings*, Berlin und Heidelberg: Springer, 240-251.

Pfitzmann, Andreas und *Hansen, Marit* (2010): *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version v 0.34 Aug. 10, 2010)*, https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v 0.34.pdf.

Ron, Dorit and *Shamir, Adi* (2013): "Quantitative Analysis of the Full Bitcoin Transaction Graph", in: Sadeghi, Ahmad-Reza (Ed.), Financial Cryptography and Data Security. 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers, Lecture Notes in Computer Science 7859, 6-24.

Schneier, Bruce (1996). *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed., Indianapolis: Wiley.

Identitätsmanagement als Grundlage von Verhaltenssteuerung

Jan Schallaböck

1 Identität

Der Begriff „Identität“ ist seit Jahren immer wieder Gegenstand der Diskussion in unterschiedlichen Kontexten. Zuletzt fanden in internationalen Standardisierungsgremien, die sich seit etwa fünf Jahren um die Entwicklung von Standards zum Identitätsmanagement bemühen, mitunter heftige Kontroversen statt.[1] Im Folgenden wird dargestellt, welche Implikationen der Begriff der Identität und seine unterschiedlichen Definitionen mit sich bringen. Daraus wird ein Lösungsvorschlag für ein weitergehendes Verständnis entwickelt.

1.1 Der Identitätsbegriff in der Logik

Ausgangspunkt des Identitätsbegriffes und oft eine zentrale Assoziationskategorie in seiner Verwendung ist die Definition aus der Logik. Leibnitz fasst es so: „Zwei Dinge sind identisch, wenn sie in allen ihren Eigenschaften ununterscheidbar sind.“[2] Abgekürzt wird dieses „Gesetz der Identität“ auch als „das Faktum, dass ein Ding es selbst ist“, oder „A=A“.

Wenn also A=A, dann hat A bestimmte Eigenschaften. Liegen diese nicht vor, dann ist es nicht A. Die bestimmten Eigenschaften sind A spezifisch inhärent, ihre Definition (bzw. Beschreibung) hingegen ist immer eine Zuschreibung. A=A, die Eigenschaften, die A bestimmen, *beschreiben* demnach nicht zwangsläufig A. Jede Eigenschaft ist, sobald wir ihr einen Namen geben, auch eine Zuschreibung. Wenn man auf eine Benennung angewiesen ist, erstellt man mit der Bestimmung von Eigenschaften

---

1 Dies kann man z.B. dem Austausch von Liaisonerklärungen zwischen ISO/IEC JTC 1/SC 27 und ITU-T SG 13 entnehmen.

2 Leibniz, Abhandlung über die Metaphysik, § 9, zit. nach Forrest 2010, dort unter Verweis auf Loemker 1969.

auch schon eine Beschreibung des Objektes. Diese Beschreibung verhält sich von der Existenz des Objekts unabhängig.

Oft besteht die Aufgabe, feststellen zu wollen, ob eine Beschreibung oder eine Eigenschaft auch tatsächlich die eines bestimmten Objekts ist. In der Feststellung dieser Übereinstimmungen liegt der Sinn der Definition von Identität. Er allerdings ist bereits jenseits des „Gesetzes der Identität", da er ohne die Beschreibung der Eigenschaften nicht auskommt.

1.2 Der Identitätsbegriff der Moderne

Die Frage der Zuschreibung von Eigenschaften zu einer Person durch andere oder auch durch die Person selbst hat insbesondere in der Psychologie eine enorme Bedeutung, strahlt aber auch auf die Soziologie und Kulturwissenschaften und nicht zuletzt auch auf das allgemeine Verständnis des Begriffes der Identität aus. Dies wird deutlich in gängigen Begriffen wie etwa der „Identitätsfindung" oder der Formulierung, dass eine bestimmte Eigenschaft „identitätsbildend" ist. Schließlich wird sogar von der Möglichkeit eines „Identitätsverlustes" gesprochen.

Der in diesen Kontexten verwendete Identitätsbegriff unterscheidet sich fundamental von einem streng logischen, obschon die dieser Begriffsverwirrung zugrunde liegenden Probleme in der philosophischen Literatur ihren Niederschlag gefunden haben.[3]

1.3 Der Identitätsbegriff der Informatik

Ausgehend von dem Begriff des „Identitätsmanagements" findet in der Informatik seit über zehn Jahren eine Diskussion um den Begriff der Identität statt.[4] Umfassende Herangehensweisen etwa bei Pfitzmann und Han-

---

3 Etwa hier: „Werden in diesem Schiff nach und nach alle Planken durch neue ersetzt, dann ist es numerisch dasselbe Schiff geblieben; hätte aber jemand die herausgenommenen alten Planken aufbewahrt und sie schließlich sämtlich in gleicher Richtung wieder zusammengefügt und aus ihnen ein Schiff gebaut, so wäre ohne Zweifel auch dieses Schiff numerisch dasselbe Schiff wie das ursprüngliche. Wir hätten dann zwei numerisch identische Schiffe, was absurd ist." (Hobbes 2012: 3).

4 Statt vieler sei auf diese Quellensammlung mit Angaben verwiesen, die bis 1998 zurück reichen: Webauftritt des Unabhängigen Landeszentrums für Datenschutz (ULD), https://www.datenschutzzentrum.de/projekte/idmanage/links.htm.

sen[5] reflektieren dabei die Differenzierungen zwischen dem logischen und dem psychologisch geprägten Begriff[6] und sind bestrebt, über eine informationstechnisch orientierte Modellierung des Begriffes eine Grundlage für Systeme insbesondere zum Umgang mit personenbezogenen Daten zu entwickeln.

In der Debatte ist jedoch erkennbar, dass dieses umfassende Verständnis oft nicht bei allen Beteiligten existiert. Vielmehr scheinen die Vorstellungen den Begriff oft lediglich auf ein „Identifikationsmanagement" zu reduzieren.[7] Diese letztgenannte Vorstellung von Identität ist dem logischen Identitätsbegriff näher. Sie blendet dabei aber nicht nur die gesellschaftliche Bedeutung und Verwendung des Begriffes, sondern letztlich auch die mit der Identifikation verbundenen gesellschaftlichen Implikationen aus. Es ist somit berechtigt zu fragen, ob der Debatte nicht ein Bärendienst erwiesen wurde, indem über den Begriff der Identität (bzw. des Identitätsmanagements) insbesondere Datenschutzaspekten stärkere Bedeutung verliehen werden sollte. Identität wird im Kontext des Identitätsmanagements oft als Sammlung von Eigenschaften verstanden, die – je nach bevorzugter Definition – zur Identifizierung ausreichend sein soll.

Allen diesen Definitionsansätzen liegt eine – für die Informatik nicht untypische – Verwechslung zwischen Bezeichner und Bezeichnetem zugrunde.[8] Dies liegt möglicherweise an einem grundlegenden Paradigma der Objektorientierten Programmierung, das versucht, die Welt (das Bezeichnete) in Objekten (die in Bezug auf diese Welt de facto Bezeichner sind) eines IT-Systems zu modellieren. So wird in unserem Fall aus der Sammlung von Eigenschaften einer Entität, also anders gesagt: der Beschreibung einer (realweltlichen) Entität, innerhalb des IT-Systems ein Objekt, das dann innerhalb dieses Systems als „Identität" bezeichnet wird. Obwohl der Begriff es nahe legt: Identisch mit dem bezeichneten Objekt ist es freilich nach keiner Definition.

Nun soll hier dem – schon aus mnemotischen Gründen sinnvollen – Paradigma der Objektorientierten Programmierung kein Generalvorwurf gemacht werden. Man kann zumindest hoffen, dass nur in sehr seltenen Fällen ein Risiko der Verwechslung von Welt und Modell, von Realität und

---

5 Pfitzmann und Hansen 2010.

6 Pfitzmann und Hansen 2010: 30 unten.

7 Etwa in Diskussionen in einschlägigen Mailinglisten wie der sogenannten „Identity Gang", mit Beiträgen von Experten der Firmen Google Inc., Verisign Inc. u.a.

8 Die freilich ausgerechnet beim Begriff „Identität" besonders absurd anmutet.

Virtualität, besteht. Konsequenterweise wird oft erkannt, dass von den „Identitäten“ innerhalb eines IT-Systems bezogen auf eine einzelne Entität in der realen Welt, eine Vielzahl existieren können, die dann oft als „partielle Identitäten“, „digitale Identitäten“, oder auch „Personas“ bezeichnet werden.

Dieses Identitätsverständnis wird nun nicht selten vermischt mit der – für die Modellierung von gesellschaftlichen Prozessen in IT-Systemen – zentralen Aufgabe der Zuordnung einer Beschreibung einer Entität innerhalb des Systems (im informatischen Sinne ist das wieder die Identität, partielle Identität oder digitale Identität) mit der Entität selber. Etwas, das in diesem Text als Identifizierung bezeichnet werden soll.

1.4 Relationale Identität als Vorschlag zur Verständigung

Will man die Vorstellungen allerdings miteinander (und mit der Wirklichkeit) versöhnen, muss – wie hier vorgeschlagen werden soll – ein alternatives Verständnis von Identität entwickelt werden. Dabei soll weitgehend auf den logischen Identitätsbegriff verzichtet werden und die Aufgabe der Beschreibung der Zuordnung von Eigenschaften zu einer Entität dem Begriff der Identifizierung überlassen werden.

Konsequent zu Ende gedacht, handelt es sich bei dem in der Informatik vertretenen Identitätsbegriff um einen relationalen Identitätsbegriff. Identifizierung ist immer eine Identifizierung von Teilidentitäten: einerseits durch die Zuordnung eines Satzes verschiedener Eigenschaften zu einem Objekt, andererseits durch die Zuordnung verschiedener Eigenschaften zur Ein- oder Ausgrenzung einer bestimmten Gruppe.

Das hier vorgeschlagene Begriffsverständnis von Identität unterstellt damit, dass Identität ein Konstrukt zwischen Entitäten ist (inklusive eines Konstruktes der Entität zu sich selbst). Die Identität ist somit die Summe solcher Eigenschaften einer Entität, die einer anderen Entität bekannt sind. Interpersonell ist die Identität einer Person also das Wissen einer anderen Person über die Person, auf die Bezug genommen wird. Eine solche Identität schließt damit – interessanterweise – auch Zuschreibungen über die Person ein, von denen der Betroffene selbst möglicherweise gar nichts weiß.

Gleichzeitig ermöglicht der Begriff zu bestimmen, welche Informationen in einem bestimmten Kontext überhaupt erforderlich sind – eine für den Persönlichkeitsschutz in der Informationsgesellschaft ausgesprochen

relevante Frage. Zu erweitern ist der Begriff schließlich im Zusammenspiel mit einer Definition des Begriffes „Entität", die klarstellen muss, dass es sich dabei nicht zwingend um ein im physischen Sinne abgrenzbares Objekt (oder eine abgrenzbare Person) handeln muss. Entität ist vielmehr eben (rekursiv) als jede Entität zu verstehen, die die Eigenschaften der Identität aufweist.

Ein Beispiel hierfür ist eine Telefonauskunft. Hierbei will der Anrufende eine Entität erreichen, die die Eigenschaft aufweist, ihm eine Telefonauskunft geben zu können. Die Identität des Objekts ist somit durch die Eigenschaft gekennzeichnet, ihm diese Auskunft erteilen zu können (oder genauer: den Dienst unter einer bestimmten Telefonnummer anzubieten). Die Verbindung zwischen dieser Identität (also vereinfacht: der Vorstellung von der Entität beim Anrufenden) und der angerufenen Entität ist damit vollständig beschrieben; auf die Unterscheidbarkeit verschiedener Mitarbeiter eines Call-Centers kommt es dabei im Normalfall nicht an.

2 Typen von Identitätsmanagement

Als eines der ersten Arbeitsergebnisse des von der Europäischen Union geförderten "Network of Excellence" FIDIS[9] entstand ein Überblick über Konzepte des Identitätsmanagements,[10] dessen Systematik auch hier als Grundlage dient. FIDIS unterscheidet drei verschiedene Typen von Identitätsmanagement:

- „Typ 1: Identitätsmanagementsysteme für das Management von (Benutzer)konten,
- Typ 2: Identitätsmanagementsysteme für das Profiling von Nutzerdaten durch eine Organisation und
- Typ 3: Identitätsmanagementsysteme für nutzerkontrolliertes kontextabhängiges Rollen- und Pseudonymmanagement"[11]

Identitätsmanagement in diesem Sinne umfasst damit eine Vielzahl von verschiedenen Perspektiven und Aufgabenstellungen. Die in FIDIS entwickelte Begriffsbildung eröffnet die Ausweitung der Forschung unter dem

---

9 Als Akronym für „Future of Identity in the Information Society", also "Zukunft der Identität in der Informationsgesellschaft".

10 Bauer et al. 2005.

11 Bauer et al. 2005: 13, Übersetzung aus dem Englischen durch den Verfasser.

Titel des Identitätsmanagements auf Datenschutztechnologien und die Einbeziehung einer Auseinandersetzung mit Profiling.

Die daraus folgende Konzentration der Datenschutzforschung auf das Identitätsmanagement ist durchaus auf Kritik gestoßen.[12] Überdies hat auch die breite Definition selbst ihre Schwächen. Sie führt zu Missverständnissen, weil viele Akteure ein auf den Typ 1 reduziertes Bild von Identitätsmanagement im Kopf haben,[13] und in der Tat fällt es schon begrifflich nicht immer leicht, ein derartig breites Konzept mit einem schillernden Begriff wie „Identität" zu vereinbaren.

Auf der anderen Seite ermöglicht die Herangehensweise eine ganzheitlichere Betrachtung, die sich von rein technischen Aufgabenstellungen, z.B. der sicheren Authentisierung von Nutzern, löst und gesellschaftliche Implikationen und technische Lösungsansätze integriert.

Im Folgenden sollen die oben genannten Typen näher erläutert werden.

2.1 Typ 1:Accountmanagement oder Identifikationsmanagement

Das Identitätsmanagement des Typs 1 ist, wie schon dargestellt, besser als Identifikationsmanagement bezeichnet. Es beschreibt die in technischen Systemen wichtige Aufgabe, einen Benutzer (nicht immer im Rahmen einer expliziten Anmeldung) durch ein System[14] wiederzuerkennen (man kann hier von Authentifizierung sprechen).[15] Vorgelagert ist die Aufgabe der Autorisierung,[16] also der Einführung eines Benutzers in ein System, und der Ausstattung mit bestimmten Rechten im System (oft auch als „Registrierung" oder „Enrollment" in eigene Teilschritte abgegrenzt). Auf dieser Grundlage kann dann die „Buchführung",[17] man könnte auch sagen, die Dokumentation des Nutzerverhaltens, im System erfolgen.

---

12 Danezis und Gürses 2010: 11.

13 Dies hat unter anderem zu intensiven Auseinandersetzungen innerhalb der Fachgremien von ISO/IEC und ITU-T geführt, wie der Verfasser selber miterleben durfte.

14 Oder eine „Domäne", vgl. Joint Technical Committee ISO/IEC JTC1, Information technology, Subcommittee SC 27, IT Security techniques 2011: 3.

15 Bauer et al. 2005: 13, differenzierter insoweit: Joint Technical Committee ISO/IEC JTC1, Information technology, Subcommittee SC 27, IT Security techniques 2011: 3.

16 Bauer et al. 2005: 13.

17 „Accounting", s. Bauer et al. 2005: 13.

Somit gilt: „Identifizierung ist eine Kernfunktion des Identitätsmanagements“[18] – zumindest für Identitätsmanagementsysteme des Typs 1. Die Identifizierung ist jedoch nur der Ausgangspunkt für nachgelagerte Prozesse oder Applikationen. Eine Identifizierung ist niemals reiner Selbstzweck.

Ergänzt wird der Prozess der Authentifizierung, also der Wiedererkennung, oft um einen weiteren Prozess, der durch den Nachweis bestimmter Eigenschaften, etwa des Alters, einer Staatsangehörigkeit oder der Zugehörigkeit zu einer Gruppe, gekennzeichnet ist. Für diesen Nachweis gegenüber der Domäne muss typischerweise ein Dritter ins Spiel kommen, weil andernfalls die reine Behauptung über das Vorliegen der Eigenschaft ausreichen und eben gerade kein Nachweis verlangt würde.[19]

Wenn im technischen System Daten über einen identifizierten Benutzer gesammelt werden, entsteht ein Profil.[20] Somit sind alle Identitätsmanagementsysteme des Typs 1 auch solche des Typs 2. Dies gilt aber nicht immer umgekehrt, wie nachfolgend dargestellt werden wird.

2.2 Typ 2: Profiling

Identitätsmanagementsysteme des Typs 2 (hier mit „Profiling“ bezeichnet) zeichnen sich dadurch aus, dass es nicht im Kern um Autorisierungen geht, sondern um die Sammlung von Daten über die Entität, etwa über eine Person. Typ 2 kann – obschon nicht immer intuitiv – mit gewissem Recht als ein Identitätsmanagementsystem verstanden werden. Die zentrale Aufgabe dieses Systems ist die Verwaltung (das Management) von Eigenschaften (Attributen) von Entitäten (Nutzern, aber auch Gegenständen), was der Definition von Identität im hier verwendeten Sinne ent-

---

18 Wie es ein Kollege im Rahmen der Vorbereitung einer Sitzung der ISO/IEC JTC 1/SC 27 WG 5 einmal ausdrückte.

19 Letzteres wird manchmal auch als „self-asserted identity“ bezeichnet.

20 Der Begriff „Profil“ selbst ist nicht immer einfach zu definieren. Als Arbeitshypothese soll hier zunächst die notwendige Bedingung zugrunde gelegt werden, dass es sich um eine Sammlung von Informationen über eine Entität handelt. Ob für eine umfassendere Definition noch weitere Kriterien hinzutreten müssen – etwa die Zeitdimension, ein gewisser Umfang oder Detailgrad von Daten – soll hier offen bleiben und hängt letztlich wohl auch vom Gebrauchskontext ab. Vgl. zu ebendiesen und dem Begriff selbst auch im Folgenden.

spricht.[21] Profiling ist dabei eine typische Anwendung, die große Praxisrelevanz aufweist, da im Wege des Profiling für den Anwender eines solchen Identitätsmanagementsystems eine Wertschöpfungskette beginnen kann, und somit ein ökonomischer Anreiz für den Einsatz besteht. Gepaart sind diese Systeme dann oft mit Anwendungen, die dem Nutzer, also der identifizierten Entität, Anreize dafür bieten, Daten für das Profiling zur Verfügung zu stellen. Beispiele für derartige Identitätsmanagementsysteme sind etwa (Teile der) Internetpräsenzen der Firmen Google Inc. oder Facebook Inc. Dabei müssen nicht zwingend bereits Daten über die Entität vorliegen. Eine Wiedererkennung (Identifikation, s.o.) kann, muss aber nicht stattfinden, wie noch zu zeigen sein wird.

Für die nachfolgenden Betrachtungen dieser Arbeit ist ein Identitätsmanagementsystem vorwiegend als Profilingsystem zu verstehen. Im Weiteren soll illustriert werden, wie verschiedene Lebensbereiche durch Identitätsmanagementsysteme dieses Typs erfasst sind.

2.3 Typ 3: Nutzerzentriertes Identitätsmanagement

Zuvor sei jedoch kurz auf den dritten Typus von Identitätsmanagementsystemen eingegangen werden. Ausgehend von Systemen des Typs 2 wird derzeit an solchen Systemen geforscht, die selbiges stärker der Nutzerkontrolle unterwerfen: Nutzerzentriertes Identitätsmanagement. Einer abschließenden Definition solcher Systeme bedarf es hier nicht, allerdings sollte das Stichwort in diesem Kontext nicht unerwähnt bleiben.

Dieser weitere Typ wird mit Typ 3, Nutzerzentriertes Identitätsmanagement (oft auch: „user-controlled“ oder „user-centric“) beschrieben. Dieser Typ stellt das Individuum, dessen Identitäten „gemanagt“ werden, ins Zentrum. Der Nutzer soll ermächtigt werden, das Management seiner Identitätsdaten in eigener Kontrolle durchzuführen und somit auch aktiv entscheiden zu können „wer was wann und bei welcher Gelegenheit” über ihn weiß.[22] Hierzu zählen insbesondere auch Funktionalitäten, die die Verwaltung von „Teilidentitäten“ ermöglichen und unterstützen, d.h. das Auftreten mit unterschiedlichen Eigenschaften, unter Umständen auch von Pseudonymen, in verschiedenen Kontexten. Diesem modernen Verständ-

21 Zur kritischen Auseinandersetzung siehe oben.
22 Vgl. BVerfGE 65, 1 (43) – Volkszählung.

nis des Identitätsmanagements liegen soziologische Konzepte wie das der „funktionalen Differenzierung“[23] oder der „kontextuellen Integrität“[24] zugrunde.

2.4 Zusammenfassung

Die hier beschriebenen Typen von Identitätsmanagementsystemen sollten nicht als abgegrenzte Taxonomie oder Partonomie verstanden werden. Sie dienen lediglich dazu, auf abstrakter Ebene verschiedene Aspekte des Identitätsmanagements deutlich zu machen. In der Praxis existieren vielfach Mischformen. Gleichzeitig zeichnen die Typen in ihrer Reihenfolge auch in etwa die chronologische Entwicklung des Identitätsmanagements nach. Entsprechend ist der Stand der Technik derzeit schon sehr weit fortgeschritten für den Typ 1, für den bereits seit vielen Jahren Industriestandards bestehen.

Für Typ 2 liegen zahlreiche Implementierungen vor, eine weitreichende Standardisierung ist allerdings noch nicht erfolgt. Ebenso ist rechtlich die Ausdifferenzierung der (offensichtlich bestehenden, durchaus diffizilen) Datenschutzanforderungen noch nicht vollständig vollzogen.

Typ 3 schließlich existiert bisher nur prototypisch oder sogar nur konzeptionell. Er ist bisher allenfalls in Teilen implementiert. Erste Ansätze weisen sowohl die Infocard-Technologie der Firma Microsoft Inc., vor allem aber das OpenID-Protokoll, allerdings mit jeweils eigenen Schwächen, auf.

Unter dem Begriff des Identitätsmanagements werden zumeist Systeme oder Systemkomponenten verstanden, die unmittelbar mit der Identifizierung (aber auch der Re-Identifizierung oder der Authentifizierung) von Entitäten befasst sind. Zunächst zählen hierzu einfache Nutzername- und Passwortsysteme. Zunehmend werden aber auch so genannte föderierte Systeme vorgefunden, die den Zugang zu Ressourcen mehrerer Organisationen einheitlich ermöglichen. Typische Beispiele für Technologien in diesem Kontext sind etwa Shibboleth, ein Protokoll, das etwa bei der Zugangskontrolle von Ressourcen des Eduroaming eingesetzt wird, oder

---

23 Luhmann 1993: 7.
24 Nissenbaum 2004.

auch wieder das OpenID-Protokoll, das bei vielen Internet-basierten Diensten weite Verbreitung gefunden hat.

Die neuere Forschung zum Identitätsmanagement will diesen Begriff dagegen (ebenso wie hier) weiter verstanden wissen als bloßes Identifikationsmanagement. Sie differenziert drei Typen des Identitätsmanagements und klassifiziert das vorgenannte enge Verständnis als Identitätsmanagement Typ I.[25] Sodann wird der Begriff des Identitätsmanagements um einen Typ II erweitert, der sich in zweierlei Hinsicht vom Typ I unterscheidet:

1. Zum Inhalt eines Identitätsmanagementsystems sollen auch solche Datenbestände zählen, die über ein Identitätsmanagement des ersten Typs mit der dort gebildeten Identität[26] verknüpft sind.
2. Weiterhin ist festzustellen, dass Identifikation nicht immer auf ein aktives Verhalten einer Entität zurückzuführen sein muss, sondern, dass oftmals auch durch Verhaltensbeobachtung oder durch technische Prozesse, die kein aktives Handeln erfordern,[27] eine Identifikation ermöglicht wird.

Aus diesen beiden Ergänzungen entsteht ein umfassenderes Verständnis des Identitätsmanagements, das auch solche Systeme umfasst, die geeignet sind, umfangreiche Profile anzulegen und zu verwalten.

3 Profilingsysteme

Im Vorangegangenen wurden verschiedene Typen von Identitätsmanagementsystemen dargestellt und der Begriff der Identität untersucht. Im Ergebnis liegt damit ein Verständnis von Identitätsmanagementsystemen als Systemen zur Speicherung und Verarbeitung von Daten über Entitäten zugrunde, wobei es unwesentlich ist, ob das System diese Entitäten selbst unterscheiden kann. Bei einer Fokussierung auf datenschutzrechtliche Aspekte sind naturgemäß solche Systeme von Interesse, in denen Daten über Menschen verarbeitet werden. Im folgenden Kapitel sollen nun anhand ei-

25 Bauer et al. 2005.

26 Freilich handelt es sich nur um eine im System vorhandene Repräsentanz einer Entität, die gerade eben nicht mit dieser identisch ist, s. aber oben.

27 Das klassische Beispiel im Onlinekontext ist die Verwendung von Cookies, siehe hierzu unten.

niger Beispiele der Einsatz solcher Systeme und die in ihnen verwendeten Mechanismen und Wirkmächtigkeiten verdeutlicht werden.

Die Verarbeitung von Daten über Menschen umfasst mittlerweile nahezu alle Lebensbereiche. Für die nachfolgende Veranschaulichung musste daher eine Selektion erfolgen. Angelehnt an die Systematik verschiedener Lebenssphären, wie sie dem Konzept des Nutzerzentrierten Identitätsmanagements zugrunde liegt, wurden hierfür drei Lebensbereiche ausgewählt. Die ersten beiden sind der Mensch als Marktteilnehmer und der Mensch in seiner sozialen Alltagskommunikation. An beiden Beispielen lassen sich einige Grundfunktionen des Identitätsmanagements gut erläutern, die auch hilfreich für die Analyse von Angriffsszenarien auf rechtlich geschützte Güter sind.

Aufgrund des besonderen Charakters von Überwachung, als einer zumeist von staatlichen Einrichtungen getragenen Aktivität, wurden diese beiden Beispiele ergänzt um einen dritten Bereich, der im Lichte der jüngeren öffentlichen Debatte die Möglichkeiten von staatlichen (Identitäts-)Überwachungssystemen unter anderem für die Abwehr von Terrorismusgefahren näher darstellt.

3.1 Der Mensch als Kunde

Kunden besser zu verstehen ist ein Teil der Marktforschung, liegt im Interesse jedes Teilnehmers an einem Bietermarkt und kann auch den Kunden selbst zugutekommen, sofern Produkte hierdurch besser auf ihre Bedürfnisse zugeschnitten werden können. Ihren Ursprung hat die Marktforschung in der empirischen Sozialforschung.[28] Sie arbeitet traditionell insbesondere mit qualitativen und quantitativen Umfragen als Primärquellen sowie mit der direkten Beobachtung.[29] Zur Marktforschung gehören somit seit jeher Identitätsmanagementsysteme in der hier unterstellten Definition.

---

28 Für eine historische Darstellung siehe etwa Wettach 2006, insbesondere S. 16.
29 Rumpel 2009: 20.

3.1.1. Statistische Verfahren

Auf Basis quantitativer Umfrageergebnisse und Beobachtungen können – bei korrekter Auswahl der Stichprobe – unter Einsatz statistischer Modelle in, im Idealfall, definierbaren Grenzen verallgemeinerbare Aussagen getroffen werden. Die Grundsystematik[30] dieser Art induktiver oder mathematischer Statistik basiert auf der Wahrscheinlichkeitstheorie, wobei „auf Basis der konkret für eine Stichprobe beobachteten Merkmalswerte jene Häufigkeitsverteilungen innerhalb der Grundgesamtheit charakterisiert (werden), mit denen das gemachte Beobachtungsergebnis in plausibler Weise erklärbar wird."[31]

Es werden somit aus der Erhebung von Stichproben (Wahrscheinlichkeits-)aussagen auf die Allgemeinheit abgeleitet. Ein vereinfachtes Beispiel mag zur Veranschaulichung für derartige Aussagen dienen: Wenn bei einer auf Repräsentativität ausgerichteten Stichprobe[32] von 1.000 Beobachteten 15%, also 150 Teilnehmer das Produkt A gekauft haben, dann ist damit zu rechnen, dass auch ungefähr 15% des Gesamtmarktes unter gleichen Bedingungen erreicht werden können. Abhängig von der Stichprobe sind dann die Aussagegenauigkeit und -wahrscheinlichkeit, die im Idealfall mit konkreten Werten belegt werden können. Im vorigen Beispiel wäre eine vollständigere Aussage: Mit einer Wahrscheinlichkeit von 95%[33]

30 Die Vielzahl der in der Marktforschung eingesetzten statistischen Verfahren und Modellierungen ist nahezu unüberschaubar. Für die Darstellung im Rahmen dieses Texts kann und muss eine vereinfachte Beschreibung genügen.

31 Wikipedia, Mathematische Statistik, http://de.wikipedia.org/wiki/Induktive_Statistik, unter „Methodik der mathematischen Statistik".

32 Eine tatsächlich repräsentative Stichprobe wird in der Praxis praktisch nie erzielt werden können, da es sich um eine echte Zufallsstichprobe handeln muss. Dies wird in der Praxis schon allein deshalb selten erreicht, weil eine zufällige Auswahl von Teilnehmern kaum erreicht werden kann. Zudem müssten alle Teilnehmer auch wirklich mitwirken und nicht etwa die Angabe verweigern. Sofern eine Zufallsstichprobe vorliegt, lässt sich aber der Grad der Repräsentativität aus der Anzahl der Grundgesamtheit und dem Hebesatz bestimmen.

33 Hier als willkürlich, aber durchaus typisch gewählter Wert zur Charakterisierung der angestrebten Aussagewahrscheinlichkeit, einführend hierzu Ludwig-Mayerhofer 2005, sehr anschaulich zur mathematischen Statistik auch Moser 2010.

würden unter bestimmten Bedingungen (denen der Stichprobe) 13–17%[34] der Marktteilnehmer das Produkt erwerben.[35]

Die Ergebnisse induktiver Statistik sind beeindruckend und beschränkt zugleich, wie an der Übereinstimmung von „Sonntagsfragen" und tatsächlichen Wahlergebnissen regelmäßig abzulesen ist. Verzerrungen und Ungenauigkeiten des Verfahrens beruhen regelmäßig darauf, dass:

1. nur eine kleine, wenig aussagekräftige Stichprobe gewählt wird, weil die Kosten großer Stichproben nicht getragen werden sollen und dass
2. bei Umfragen nicht tatsächliches Verhalten, sondern nur subjektive Äußerungen zu möglichem oder projiziertem Verhalten erfasst werden, das tatsächliche Verhalten aber in nicht prognostizierbarer Weise anders ausfallen kann.[36]

3.1.2. Cross-site-tracking und targeted advertising

Die Beziehung zwischen Kunden und Händler stellt sich im Internet genau in Bezug auf die beiden vorgenannten Punkte grundsätzlich anders dar. Durch den Einsatz von „cross-site-tracking" ist Marktforschung möglich,

---

34 Bei einer Aussagegenauigkeit von +–2%, die von der Größe der Stichprobe in Abhängigkeit von der Größe der Grundgesamtheit bestimmt wird.

35 In einem juristisch ausgerichteten Text kann man es wohl nicht deutlich genug sagen: statistische Aussagen sind *nicht* geeignet, um Einzelfallgerechtigkeit herzustellen. Im oben genannten einfachen Beispiel mit einer Eintrittswahrscheinlichkeit von 95% ergibt sich im Umkehrschluss, dass mit einer Restwahrscheinlichkeit von 5% - also in jedem 20. Fall – das Ereignis nicht eintritt, die Aussage falsch ist etc. Es handelt sich um Typisierungen, deren Heranziehung nach allgemeiner Ansicht wohl verfassungsrechtlich etwa auch im Bereich des Verwaltungshandelns (aber nicht in strafrechtlichen Entscheidungen) zulässig sein dürfte, eingehend Stockter 2008: 332 ff. m.z.w.N. in Bezug auf die generelle Zulässigkeit von Typisierungen, wobei die Gleichsetzung statistischer mit anderen Typisierungen m.E. für die zahlreichen Fälle fehlender hermeneutischer Erklärungsmuster, das heißt fehlender inhaltlich-sachlicher Begründungszusammenhänge, durchaus noch einmal weiter hinterfragt werden könnte. Dies gilt umso mehr, als zunehmend komplexe multifaktorielle Verfahren zum Einsatz kommen, die kaum noch hermeneutisch zu durchdringen sind.

36 Wahlbefragungen werden daher in der Regel an bestimmten Stellen korrigiert („gewichtet"), weil man etwa aus Erfahrung weiß, dass Wähler extremer Parteien in einer Befragung ihr tatsächliches Wahlverhalten nicht angeben, siehe hierzu etwa Kunert 2013.

die ausschließlich auf Beobachtungsdaten aufbaut und gleichzeitig Stichproben ermöglicht, die nahezu die Eigenschaften einer Vollerhebung aufweisen, wodurch die oben bezeichneten Fehlerquellen massiv reduziert werden können. Gleichzeitig ermöglichen Verfahren wie das des „targeted advertising“ zusätzlich eine direktere Ansprache solcher Nutzer, bei denen ein hohes Kaufpotential identifiziert wurde.

„Cross-site-tracking“ ist ein Verfahren, das es dem Betreiber des Systems ermöglicht, einen Nutzer über mehrere Seiten zu „verfolgen“ (engl. „tracken“). Einfache Verfahren beruhen dabei auf dem Einsatz eines so genannten „Cookies“ durch jede besuchte Seite unter Mitwirkung des jeweiligen Seitenbetreibers. Dabei wird zumeist eine Datei mit einer Identifikationsnummer auf dem Computer des Nutzers hinterlegt, die unter bestimmten Bedingungen wieder ausgelesen wird. Der Betreiber des Trackingsystems erkennt darüber Nutzer (genauer: die Identifikationsnummern des Cookies, die von deren Internetbrowsern übermittelt werden) beim Besuchen jeder mitwirkenden Webseite wieder und kann so ein Interessenprofil des einzelnen Nutzers erstellen.[37] Neben Cookies lassen sich eine Vielzahl von anderen Mechanismen zur Re-Identifikation des Browsers oder Nutzers einsetzen, wobei diese – anders als bei Cookies – vielfach für den Nutzer nicht mehr kontrollierbar oder überhaupt feststellbar sind.[38] Mittels „cross-site-tracking“ kann das Verhalten eines Nutzers auf allen einbezogenen Internetseiten nachvollzogen werden. Im Extremfall entsteht ein vollständiges Profil des Rezeptions- und Nutzungsverhaltens im Internet. Zusätzlich können fallweise auch Daten aus anderen Diensten verknüpft werden und in ein Nutzungsprofil einfließen.[39] Für die Marktforschung von besonderem Interesse ist dabei naturgemäß die Verknüpfung mit dem Kaufverhalten. So kann bei entsprechender Modellierung über die vorhandenen Daten festgestellt werden, dass die Nutzer bestimmter Seiten eine besondere Affinität zu einem bestimmten Produkt haben.

---

37 Vgl. Hansen et al. 2007: 191 ff. Im Rahmen dieser Untersuchung wurde bereits 2007 dargestellt, dass einer der damaligen Marktführer für dieses Verfahren, die Firma Doubleclick Inc., Kooperationsvereinbarungen mit nahezu allen großen deutschen Nachrichtenportalen vorweisen konnte.

38 Für einen Überblick siehe Schoen 2009, ebenfalls übersichtlich bei Dimov 2013 sowie bei Mittal 2010: 10 ff., wenngleich weniger umfassend.

39 Siehe hierzu ebenfalls Hansen et al. 2007: 191 ff.

Durch „targeted advertising“ schließlich soll es möglich sein, potentielle Kunden mit bestimmten Eigenschaften auch gezielt zu erreichen. Hierbei wird aus dem Internetnutzungsverhalten statistisch auf bestimmte Eigenschaften, etwa Hobbys oder Interessen zurückgeschlossen und der Nutzer aufgrund dieser Eigenschaften gezielt mit Werbung „beschossen“.[40] Die Verfahren zur automatisierten Entscheidung darüber, wer welche Werbung erhält, kann man wohl zumeist als Scoring-Verfahren beschreiben.[41]

3.1.3. Scoring

Wohl von allen statistischen Verfahren im Umgang mit persönlichen Daten am besten diskutiert sind so genannte Scoringverfahren,[42] insbesondere das Kreditscoring.[43] Da sie bereits besser in öffentlich verfügbaren Studien analysiert sind als das „targeted advertising“, eignen sie sich besonders als Diskussionsgrundlage. Beim Kreditscoring werden die abstrakt schon oben beschriebenen Verfahren eingesetzt, um insbesondere das Ausfallrisiko eines potentiellen Kredits zu bewerten. Dabei werden – vereinfacht gesagt – bisherige Erfahrungswerte aus dem Kundenstamm der Bank, oft unter Hinzuziehung fremder Datenbestände, zunächst zu bereits erfolgten Kreditausfällen in Beziehung gesetzt, wobei hier Korrelationsverfahren eingesetzt werden.[44] Dann wird unter Nutzung der verfügbaren Einzelangaben eines Kreditinteressierten das statistische Kreditausfallrisiko im konkreten Fall abgeleitet.[45]

---

40 „To target“, engl. für zielen, „advertising“, engl. für Werbung, also „gezielte Werbung“.

41 Im Sinne der Beschreibung bei Kamp und Weichert 2005: 10; im Detail dazu nun im Folgenden.

42 Umfassend schon, wenngleich unter Hinweis auf die immer noch unklare Tatsachenlage: Kamp und Weichert 2005, etwa auf S. 24 und 45, grundsätzlich kritisch: Schallaböck und Damm 2005: 10.

43 Zu neueren Verfahren s. Bröker 2010: 83ff.

44 Vgl. für das dort beschriebene System etwa Typke 2009: 9, oder auch wieder Kamp und Weichert 2005: 10 m.w.N. Korrelationsverfahren stellen fest, ob ein mathematischer Zusammenhang zwischen zwei Werten besteht.

45 Neben dem reinen unternehmensinternen Scoring kommt natürlich insbesondere dem Scoring über Unternehmensgrenzen und unter Rückgriff auf Informationen aus einer Vielzahl von Unternehmen eine relevante Rolle zu. Dieser Fall wurde hier aus Gründen der Vereinfachung jedoch nicht vertieft, da er in Bezug auf den Mechanismus keine Besonderheiten aufweist.

Scoring-Verfahren können in verschiedensten Bereichen zur Prognose menschlicher Verhaltensweisen eingesetzt werden. Neben der bereits erwähnten Verwendung im Bereich des „targeted advertising“ kann man beim Verbraucher-Scoring verschiedene Typen des Werbe-Scoring und des Vertrags-Scoring unterscheiden. Darüber hinaus kann man den Einsatz im Bereich der inneren Sicherheit und der gesetzlichen Krankenversicherung (hier, um „individuelle Kosten- und Leistungsparameter“ festzulegen), in Betracht ziehen.[46] Schließlich könnte man sicherlich auch den Einsatz im Vorfeld von Wahlen erwägen, um gezielter auf Wechselwähler zuzugehen.[47] Letztgenanntes Beispiel weist bereits deutlich auf die unmittelbaren Effekte für die Demokratie hin, indem man sich verdeutlicht, wie es sich in diesem Zusammenhang auswirken könnte, wenn die entsprechenden Verfahren nicht allen Parteien gleichermaßen zur Verfügung stehen.

3.2 Der Mensch und seine Alltagskommunikation

Nachdem im Vorangegangen exemplarisch dargestellt wurde, wie Identitätsmanagementsysteme in Kundenbeziehungen eingesetzt werden können und eingesetzt werden, sollen im Folgenden die Profilbildungsmöglichkeiten auf der Basis netzbasierter Alltagskommunikation aufgezeigt werden.[48] Anders als im obigen Abschnitt soll hier nicht so sehr die Auswertung im Vordergrund der Darstellung stehen, sondern die Möglichkeit der Sammlung von Informationen. Es wird sich zeigen, dass jenseits der unmittelbaren Kommunikation, neudeutsch: „face to face“, umfassende, nahezu vollständige Kommunikations- und Sozialprofile entstehen.

Eines der ältesten Protokolle des Internet, das heute noch große Relevanz besitzt ist, ist der aus dem aus Jahr 1982 stammende „Standard for the Format of ARPA Internet Text Messages“,[49] der trotz mehrfacher Ak-

46 Kamp und Weichert 2005: 11 ff.

47 Vgl. Issenberg 2012 mit einer Darstellung über den Einsatz von Scoringverfahren bei den US-Präsidentschaftswahlen im Jahr 2012.

48 Der Begriff der Alltagskommunikation ist in jüngster Zeit immer wieder als Grundlage für Überlegungen zu einem Abgrenzungskriterium für die Anwendung von Datenschutzrecht herangezogen worden, vgl. Lutterbeck 2013: 2 unter Verweis auf neun, wohl im direkten Gespräch formulierte Thesen von Jochen Schneider. Etwas differenzierter allerdings Schneider (2011: 238) selbst.

49 Crocker 1982.

tualisierungen[50] wohl immer noch als Grundlage für die heutige Kommunikation per E-Mail bezeichnet werden kann. E-Mail ist immer noch einer der wichtigsten und am meisten verbreiteten Dienste im Internet. Allerdings gewinnen in letzter Zeit neben Diensten, die eher auf den Austausch kurzer Nachrichten ausgerichtet sind,[51] vor allen Dingen der Nachrichtenaustausch in sozialen Netzwerken, an Bedeutung.[52]

Den verschiedenen Kommunikationsdiensten ist gemein, dass neben dem Inhalt der Nachricht Informationen über den Zeitpunkt einer Kommunikation sowie über Sender und Empfänger entstehen.[53] Bei den Diensten von Facebook Inc. und Twitter Inc. sind diese Informationen für alle durchgeführten Nutzungen in ihrem jeweiligen System hinterlegt. Je nach Nutzungsverhalten können somit nicht nur umfassende individuelle Kommunikationsprofile, sondern auch Profile über ganze Kommunikationsnetzwerke entstehen. Aber auch bei dem – distribuierten, weil offen spezifizierten – Dienst E-Mail liegt wegen der verbreiteten Nutzung entsprechender Diensteanbieter (anstelle eines eigenen Servers) bei diesem ein recht umfassendes individuelles Kommunikationsprofil vor. Aufgrund der nicht unerheblichen Marktkonzentration auf wenige große Anbieter liegen bei diesen eine enorme Zahl individueller Kommunikationsprofile vor, die in ihrer Summe unter Umständen große Teile von Kommunikationsnetzwerken abbilden können. Ähnliche Profile entstehen im Übrigen auch in den Infrastrukturen der Telefonkommunikation. Auch hier liegen umfassende Kommunikationsprofile bis hin zu Profilen von Kommunikationsnetzwerken vor.

Gerade die Analyse von Kommunikationsnetzwerken ermöglicht wiederum ausgesprochen relevante Auswertungen. So kann die Auswertung interner E-Mail-Kommunikationsstrukturen am Arbeitsplatz mit tatsächlichen Organisationsstrukturen verglichen werden, um Ähnlichkeiten und Unterschiede zu erkennen. Unter Umständen lässt sich hierbei in Kombi-

---

50 Resnick 2001: 1 und 2008: 1.

51 Zu denken ist hier derzeit neben „internet chats“, etwa über „Internet-Relay-Chats“ (IRC) oder Jabber mit seiner XMPP-Protokollfamilie (für eine Übersicht: Peter 2013) an den Kurznachrichtendienst twitter der Firma Twitter Inc.

52 Vgl. Bausch und McGiboney 2009: 1ff. Die Umstellung auf Facebook für Universitäten überlegend: Whittaker 2009.

53 Dies ist systemimmanent ersichtlich und ergibt sich für E-Mail spezifisch aus Resnick 2008: 22 f.

nation mit statistischen Verfahren wohl sogar die Wahrscheinlichkeit eines zukünftigen Jobwechsels errechnen.[54]

3.3 Der Mensch als Terrorist: staatliche Überwachung

Nachdem im Vorangegangenen Datensammlungen in der Kommunikation von Bürgern untereinander und in Beziehungen zwischen Bürger und Unternehmen dargestellt worden sind, soll nun das Verhältnis zwischen Staat und Bürger näher betrachtet werden. Dabei kann man nicht umhin, auch und insbesondere die Enthüllungen des US-amerikanischen Whistleblowers Edward Snowden in den Fokus zu nehmen. Für die weitere Argumentation sind diese Enthüllungen aber nicht so sehr deswegen relevant, weil sie tatsächlich wahr sein könnten,[55] sondern weil sie und die sie umgebende Debatte deutlich machen, was technisch möglich ist.

Die öffentliche Debatte der vergangenen Jahre hatte sich im Wesentlichen noch auf die Fragen staatlicher Zugriffsbefugnisse auf und Speicherpflichten für Daten privater Diensteanbieter insbesondere im Rahmen der so genannten Vorratsdatenspeicherung konzentriert. Im Lichte der Enthüllungen von Edward Snowden erscheinen diese Auseinandersetzungen wie ein Streit um Petitessen. Das darf aber nicht darüber hinweg täuschen, dass die oben beschriebenen Kommunikationsnetzwerke durch die Vorratsdatenspeicherung in staatlichen Zugriff geraten. Durch Zugriff auf diese Daten, der unterdessen auch weitgehend automatisiert erfolgt,[56] kann man das Gesamtsystem der Vorratsdatenspeicherung als ein staatliches Identitätsmanagementsystem zur Vorhaltung von Kommunikationsdaten beschreiben.[57]

---

54 Rieger 2010.

55 Wovon nach Einschätzung des Verfassers im Übrigen aber auszugehen ist. Die deutsche Bundesregierung misst den Enthüllungen nach wie vor nicht den erforderlichen Stellenwert zu, obschon auch das Handeln der US-amerikanischen Regierung allein aufgrund ihres Mangels an Dementis eigentlich keinen Zweifel an der Echtheit der veröffentlichten Dokumente entstehen lassen dürfte.

56 In ETSI 2009 wird ein solcher automatischer Zugriff spezifiziert.

57 Interessant ist allerdings bei diesem Verständnis einer Gesamtarchitektur, dass ihre Ausgestaltung eine Separierung zwischen Staat und Providern vorsieht, die mögliche Auswertungen bestimmt. Eine Auswertung des bei den Providern vorliegenden Gesamtbestands der Daten ist nämlich nur noch möglich, wenn auch alle diese

Die Identitätsmanagementsysteme, die augenscheinlich von den US-amerikanischen und britischen Geheimdiensten NSA bzw. GCHQ betrieben werden, sind allerdings erheblich umfassender und ermöglichen weit mehr, als nur den Zugriff auf Kommunikationsbeziehungen einzelner. Es erscheint sogar möglich, dass die gesamte netzbasierte Kommunikation dauerhaft gespeichert wird, sofern sie einen der zahlreichen möglichen Zugriffspunkte durchläuft.[58] Neben solcherlei „Internet-Rohdaten"[59] sollen an einer Vielzahl von Stellen auch gezielte Zugriffe auf Datenbestände großer Diensteanbieter in ihrer jeweiligen systemspezifischen Semantisierung erfolgen, was einem Zugriff auf die vollständigen Kommunikationsdaten zumindest nahe käme.[60]

Von besonderem Interesse sind aber gerade auch die oben bezeichneten „Internet-Rohdaten". Zunächst könnte die Frage aufgeworfen werden, ob diese Daten überhaupt der Definition eines Identitätsmanagementsystems genügen können, wieso sie hier also Gegenstand der Betrachtung sind. Anders – an der Definition orientiert – gefragt: Wie kann denn eine Zuordnung der Daten zu einer Entität überhaupt vorliegen? Dies ergibt sich jedoch relativ unproblematisch, wenn man sich verdeutlicht, dass es sich bei diesen Rohdaten definitorisch – denn es handelt sich um eine Speicherung von Internet-Rohdaten – um Daten gemäß dem Internet Protokoll handelt, womit schon auf einer ersten Analyseebene die Absender- und Empfänger-IP-Adresse eines Paketes vorliegen. Somit können alle weiteren Daten

---

Daten vorher systematisch abgefragt werden, oder eine Übertragung jenseits des in ETSI 2009 bezeichneten Protokolls stattfindet.

58 Die Berichterstattung scheint zurzeit zumindest eine temporäre Speicherung der Gesamtkommunikation im oben verstandenen Sinne nahe zu legen, vgl. MacAskill et al. 2013, Hinweise hierauf und auf den Einsatz von DPI (s.u.) in diesem Kontext schon in Singel 2006. Die nach Bamford 2012 entstehenden Speicherkapazitäten der NSA im US-Bundesstaat Utah lassen rechnerisch auch eine dauerhafte Vollspeicherung nicht als ausgeschlossen erscheinen.

59 Im englischen spricht man von „internet traffic data", was sich aber gerade nicht mit der Legaldefinition des eigentlich naheliegenden Begriffes „Verkehrsdaten" des § 3 Nr. 30 TKG deckt. Anders als bei letztgenannten handelt es sich bei ersteren nicht um einen beschränkten, definierten Satz an Datentypen, sondern um den gesamten Datenbestand, der durch eine physikalische Verbindung übermittelt wird.

60 Diesbezüglich ist es allerdings möglich, dass ein unmittelbarer Zugriff auf den Gesamtdatenbestand nicht stattfindet, sondern zunächst eine Entscheidung durch ein Gericht üblich ist.

als Eigenschaften einer Entität mit besagter IP-Adresse beschrieben werden.

3.3.1. Deep Packet Inspection

Von Bedeutung ist die Frage, wie und welche Datenbestände tiefergehend extrahiert werden können. Bei den hierfür verfügbaren und eingesetzten Verfahren spricht man von „Deep-Packet Inspection“ (DPI).[61]

Es ist theoretisch wohl möglich, aus diesem Datenbestand sämtliche Kommunikationsinhalte zu extrahieren. Dies gilt zumindest, sofern die verwendeten Protokolle bekannt sind und die Daten nicht oder dechiffrierbar verschlüsselt sind.[62] Damit besteht zumindest ein theoretisches Potential, dass durch das Speichern der Rohdaten das gesamte Internetnutzungsverhalten aller Menschen analysiert werden kann. Die veröffentlichten Darstellungen zur Praxis einiger Geheimdienste legen darüber hinaus nahe, dass dies zu einem nicht unerheblichen Teil auch tatsächlich erfolgt.

Anders, als es beispielsweise Joffe suggeriert,[63] ist dabei das Problem des „information overload“ ein überschätztes Problem. Der (gerne wiederholte) Hinweis auf ein Zuviel an Informationen, das es schwierig mache, die sprichwörtliche „Nadel im Heuhaufen“ zu finden, droht, von den tatsächlich vorliegenden Problemen abzulenken. Entscheidend ist vielmehr, dass in der Tat auf Basis der Datenbestände vermeintliche oder tatsächliche Erkenntnisgewinne gezogen werden, die später auch handlungsleitend sein können. Dass man mit solcherlei Datenbeständen nicht jedem denkbaren Ziel gerecht wird, liegt auf der Hand, ist aber – wie gesagt – unwesentlich.

---

61 „Tief gehende Paketanalyse“, zur Technologie selbst und der rechtlichen Zulässigkeit typischer Verfahren in Deutschland s. Bedner 2009. Die öffentliche Debatte und Forschung konzentrieren sich dabei allerdings hauptsächlich auf Fragen der Netzneutralität, da ein typisches Einsatzszenario die Analyse von Verbindungen mit anschließender Diskriminierung bestimmter Diensttypen, wie etwa filesharing, darstellt. Statt vieler und bereits mit deutlichem Hinweis auf das („disruptive“) Überwachungspotential: Bendrath 2009.

62 Zu dieser Einschätzung kommt richtigerweise Parsons 2009: 1, 8 mit weiteren Quellen für das Beispiel der Zusammenführung von E-Mails über den Dienst der Firma Google Inc.

63 Joffe 2013.

3.3.2. Mustererkennungsverfahren

Die nächste Frage, die sich ergibt, ist die nach den Auswertungsmöglichkeiten der Datenbestände. Dabei kommt neben den schon oben bezeichneten Verfahren wohl Mustererkennungsverfahren eine besondere Rolle zu. Gegenstand näherer Betrachtung sollen hier insbesondere Methoden sein, die künstliche neuronale Netze einsetzen, weil diese einige interessante und relevante Charakteristika aufweisen, auch wenn zahlreiche andere Mustererkennungsverfahren möglicherweise in der bekannten Praxis eine höhere Relevanz aufweisen.[64]

Künstliche neuronale Netze erlauben, inspiriert durch Annahmen über Funktionsweisen des Nervensystems des Gehirns,[65] Beziehungen zwischen zwei Eigenschaften mittels selbstlernender Mechanismen[66] zu ermitteln. Die konkreten eingesetzten Verfahren künstlicher neuronaler Netze sind vielfältig.[67] Gemein ist ihnen, dass sie auf der Vernetzung oder Verbindung einer großen Zahl einzelner Funktionen, sog. "Neuronen", basieren.[68] Im Rahmen des Lernprozesses des künstlichen neuronalen Netzwerkes werden nun die Verbindungen dieser Funktionen verändert (in einfachen Fällen durch Löschen oder Hinzufügen), sodass im Idealfall das künstliche neuronale Netzwerk aus gegebenen Eingabeparametern das antizipierte Ergebnis produziert. Dabei wird – vereinfacht gesprochen – typischerweise ein richtiges Ergebnis durch Verstärkung der Verbindung belohnt, ein falsches durch Abschwächung bestraft.[69] Ist das Netzwerk hinreichend trainiert, kann es auf Eingabewerte angewendet werden, ohne dass das Ergebnis bekannt ist.

---

64 Zu denken wäre hier beispielsweise an Bayes'sche Filter, die erfolgreich zur Erkennung von Spam E-Mails eingesetzt werden, s. Graham 2002.

65 Rojas 1996: 4.

66 Wobei hier zwischen verschiedenen Lernverfahren, etwa dem überwachten und dem unüberwachten Lernen unterschieden wird, vgl. Rojas 1996: 78.

67 Für eine Übersicht siehe etwa: Wikipedia, Künstliches neuronales Netz, https://de.wikipedia.org/wiki/K%C3%BCnstliches_neuronales_ Netz#Lernverfahren, im Abschnitt „Klassen und Typen von KNN".

68 Rojas 1996: 29 f.

69 Man spricht bei dieser Kombination des Neurons und seiner Verbindungen auch von einem „gewichteten Perzeptron", vgl. Rojas 1996: 55 ff.

Die Aufgabenstellung neuronaler Netzwerke ist mithin dieselbe wie bei den oben beschriebenen Scoringverfahren.[70] Es soll aus einer Reihe von Eingabewerten auf einen (oder mehrere) Ausgabewerte (im Fall des Kreditscorings beispielsweise auf das Zahlungsausfallrisiko) geschlossen werden. Anders als bei einer Vielzahl der oben beschriebenen Scoringverfahren, sind die Mechanismen, die zu dem Ergebnis führen, in der Regel nicht oder kaum mehr identifizierbar. Man spricht auch von einem „Black-Box System", also einem System, dessen Funktionsweise nicht erkennbar ist. Dies liegt daran, dass sich die Funktionsweise eines neuronalen Netzwerkes erst aus dem Zusammenspiel einer Vielzahl der antrainierten Verbindungen ergibt.[71] Hinzu kommt, dass künstliche neuronale Netzwerke auch so konzipiert werden können, dass sie sich ständig weiter entwickeln, was die Schwierigkeit erhöht, festzustellen, was im Einzelfall zu einem bestimmten Ergebnis geführt hat.

Chinesische Forscher untersuchen seit einiger Zeit die Einsetzbarkeit künstlicher neuronaler Netzwerke bei der Deep Packet Inspection, um bestimmte Applikationen zu identifizieren.[72] Ziel solcher Forschung kann es sein, solche Daten zu erkennen (in der Regel mit dem Ziel, diese auszufiltern oder zu verzögern), die im Wege von so genannten „p2p-filesharing-Netzwerken" ausgetauscht werden.[73] Aber es werden auch andere Einsatzfelder betrachtet. Andernorts wird beispielsweise untersucht, wie mittels künstlicher neuronaler Netze Börsenkurse besser prognostiziert werden könnten.[74] Schließlich existieren seit kurzem Modelle zur Analyse der Grundstimmung von Texten, der sogenannte Sentiment-Analyse, die eine Genauigkeit von bis zu 85% erreichen kann. So kann zum Beispiel maschinell ausgewertet werden, ob Kommentierungen zu Filmen, die von Nutzern einer entsprechenden Plattform abgegeben wurden, überwiegend positiv oder negativ sind.[75]

---

70 Künstliche neuronale Netzwerke können durchaus auch in ein Scoringmodell integriert werden. Für eine umfassendere Typisierung siehe Kamp und Weichert 2005: 56, für einen Überblick über Verfahren für Data-Mining: Wu et al. 2008.

71 Chorowski und Zurada 2011; Augasta und Kathirvalavakumar 2012: 2 unter Verweis auf Mantas et al. 2006: 1, jeweils allerdings auch schon mit Darstellungen von Ansätzen, aus künstlichen neuronalen Netzen wieder Regeln zu extrahieren.

72 Tan, Jun et al. 2012: 2218 m.z.w.N.

73 So z. B. bei Agrawal und Sohi 2011.

74 Kara et al. 2011, auch schon mittels einfacher Korrelationsanalyse: Preis et al. 2013.

75 Socher 2013: 1.

Denkbar ist eine Vielzahl weiterer Einsatzszenarien, vorausgesetzt, es liegen jeweils hinreichend große Trainingsdatenbestände vor. Diese sind wohl bei Vollerfassungen der Internet-Rohdaten in vielerlei Dimensionen gegeben. Allein, es gibt keine gesicherten veröffentlichten Kenntnisse darüber, wie diese Informationen derzeit in Profilen angereichert werden, oder welche konkreten Informationen gewonnen werden. Die vorliegenden Hinweise sollten aber gezeigt haben, dass hier grundsätzlich erhebliche Möglichkeiten bestehen dürften. Ob diese jedoch gerade für die Ermittlung von Terroristen besonders geeignet sind, ist zweifelhaft, da hierfür – aufgrund deren geringer Zahl – keine umfangreichen Trainingsdaten vorliegen dürften.[76]

4 Zusammenfassung

Zusammenfassend ist festzustellen, dass durch die Nutzung von sehr umfassenden Datenbeständen der Trend zu weitreichender Analyse menschlicher Verhaltensweisen ungebrochen voranschreitet. Über das genaue Ausmaß der Möglichkeiten, die diese Analysen bieten, kann nur vage spekuliert werden. Eine umfassende wissenschaftliche Aufarbeitung – etwa unter dem Gesichtspunkt einer „Überwachungs-Gesamtrechnung“[77] – besteht nicht. Deutlich wird aber, dass der Datenbestand, der für solcherlei Analysen genutzt werden könnte, Ausmaße angenommen hat, die in einigen Lebensbereichen einer Art Vollüberwachung gleichkommen. Es wurde gezeigt, dass die Datenbestände durchaus ausgewertet werden können. Dies scheitert in aller Regel nicht daran, dass sie nicht verfügbar wären, oder nicht zusammen geführt werden können – auch wenn dies gerne behauptet wird.

Es wurde gezeigt, dass solche Analysen nur auf der Grundlage eines Datenbestands über bestimmte einzelne Entitäten möglich sind. Auf der anderen Seite können die Informationen, die durch Erhebung bei anderen Personen gefunden werden, auf eine Person zurückwirken. Mit anderen Worten: Auch wenn eine bestimmte Information bei einer Person gar nicht erhoben wurde,[78] kann sie gegebenenfalls als statistische Information – als

---

76 Insoweit ähnlich in Bezug auf den Einsatz Bayes’scher Filter: Chivers 2013.

77 Roßnagel 2010.

78 Und manchmal auch nicht erhoben werden kann, weil sie sich auf prognostische Sachverhalte bezieht.

Wahrscheinlichkeitsaussage über eine Person – dennoch erzeugt werden und somit vorliegen. Es besteht insoweit eine Art Drittbetroffenheit bei der Erhebung personenbezogener Informationen. Wirtschaftswissenschaftlich handelt es sich um Externalisierungseffekte der Transaktionen zwischen den Parteien. Hieraus kann man wohl durchaus den Schluss ziehen, dass in der Art, wie Identitätsmanagement praktiziert wird, erhebliche Potentiale liegen, steuernd auf Menschen einzuwirken.

Insbesondere die vorbezeichnete Drittbetroffenheit wirft eine Vielzahl von neuen Fragen auf. Sie konfligiert mit dem zentralen Paradigma des Datenschutzrechts – der Einwilligung. Personenbezogene Daten scheinen nämlich nicht in dieser Form transaktionsfähig zu sein. Die Einwilligung, die ein Betroffener erteilen mag, hat eventuell Rückwirkungen auf einen anderen, der niemals eine Einwilligung erteilt hat.

Es liegt nahe, die Frage nach dem „qui bono" zu stellen – und de lege ferenda auch die Frage „wem *sollte* es nützen". Dabei darf keinesfalls übersehen werden, dass Externalisierungen auch positiver Natur sein können. Ein umfassendes Verständnis über menschliche Verhaltensweisen und Mechanismen zur Verhaltenssteuerung kann zum Beispiel durchaus Grundlage von „good governance" sein. Zweifelhaft ist allerdings, ob es zielführend ist, die Frage danach, wer – möglicherweise sogar exklusiv – auf derartiges Wissen zugreifen kann, dem freien Spiel der Kräfte zu unterwerfen.

Literatur

Agrawal, Sunil and *Sohi, Balwinder* S. (2011): „Generalization and Optimization of Feature Set for Accurate Identification of P2P Traffic in the Internet using Neural Network", in: *WSEAS TRANSACTIONS on COMMUNICATIONS* 19(2), 55-65, http://www.wseas.us/e-library/transactions/communications/2011/52-578.pdf.

Augasta, M. Gethsiyal and *Kathirvalavakumar, Thangairulappan* (2012): „Reverse Engineering the Neural Networks for Rule Extraction in Classification Problems", in: *Neural Processing Letters*, 35(2), 131-150, http://dx.doi.org/10.1007/s11063-011-9207-8.

Bamford, James (2012): *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, http://www.wired.com/2012/03/ff_nsadatacenter/.

Bauer Matthias, Meints Martin und *Hansen Marit* (2005): *FIDIS Deliverable 3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems*, http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf.

Bausch, Suzy und *McGiboney, Michelle* (2009), *News Release: SOCIAL NETWORKS BLOGS NOW 4TH MOST POPULAR ONLINE ACTIVITY, AHEAD OF PERSONAL EMAIL, NIELSEN REPORTS. 'Time Spent' on These Sites Growing Three Times Faster than Overall Internet Rate, Now Accounting for Almost 10 Percent of all Internet Time*, http://www.nielsen-online.com/pr/pr_090309.pdf.

Bedner, Mark (2009): *Rechtmäßigkeit der „Deep Packet Inspection"*, http://kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf.

Bendrath, Ralf (2009), *Global technology trends and national regulation: Explaining Variation in the Governance of Deep Packet Inspection*, http://userpage.fu-berlin.de/bendrath/Paper_Ralf-Bendrath_DPI_v 1-5.pdf.

Bröker, Frank (2010): „Neue Trends beim Kreditscoring natürlicher Personen", in: Brunner Wolfgang, Seeger Jürgen und Turturica, Willi (Hrsg.), *Fremdfinanzierung von Gebrauchsgütern. Das alltägliche Risiko*, Wiesbaden: Gabler Verlag, 83–97, http://dx.doi.org/10.1007/978-3-8349-8961-1_6.

Chivers, Corey (2013): *How likely is the NSA PRISM program to catch a terrorist?*, http://bayesianbiologist.com/2013/06/06/how-likely-is-the-nsa-prism-program-to-catch-a-terrorist/.

Chorowski, Jan and *Zurada, Jacek M.* (2011): „Extracting Rules From Neural Networks as Decision Diagrams", in: *IEEE Transactions on Neural Networks* 22(12), 2435–2446.

Crocker, David H. (1982): *RFC 822 - STANDARD FOR THE FORMAT OF ARPA INTERNET TEXT MESSAGES*, http://tools.ietf.org/pdf/rfc822.pdf.

Danezis, George und *Gürses, Seda* (2010): *A critical review of 10 years of Privacy Technology*, http://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf.

Dimov, Ivan (2013): *Means and Methods of Web Tracking: Its effects on privacy and ways to avoid getting tracked*, http://resources.infosecinstitute.com/means-and-methods-of-web-tracking-its-effects-on-privacy-and-ways-to-avoid-getting-tracked/.

European Telecommunications Standards Institute (ETSI) (2009): *ETSI 102 657 - V1.3.1 - Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data*, http://www.etsi.org/deliver/etsi_ts/102600_102699/102657/01.03.01_60/ts_102657v 010301p.pdf.

Forrest, Peter (2010): *The Identity of Indiscernibles*, http://plato.stanford.edu/entries/identity-indiscernible/.

Graham, Paul (2002): *A Plan for Spam*, http://www.paulgraham.com/spam.html.

Hansen Marit, Hansen Markus, Häuser Marita, Janneck Kai, Krasemann Henry, Meints Martin, Meissner Sebastian, Raguse Maren, Rost Martin, Schallaböck Jan, Clauß Sebastian, Steinbrecher Sandra und *Pfitzmann Andreas* (2007): *Verkettung digitaler Identitäten*, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/projekte/verkettung/.

Hobbes, Thomas (2012): *Grundzüge der Philosophie* (Erweiterte Ausgabe), Altenmünster: Jazzybee Verlag.

Issenberg, Sasha (2012): *How President Obama's campaign used big data to rally individual voters*, http://www.technologyreview.com/featuredstory/509026/how-obamas-team-used-big-data-to-rally-voters/.

Joffe, Josef (2013): *Nadel und Heuhaufen. Europäer und Amerikaner – gemeinsam den Schnüffelstaat stoppen*, http://www.zeit.de/2013/30/nsa-europa-schnueffelstaat

Joint Technical Committee ISO/IEC JTC1, Information technology, Subcommittee SC 27, IT Security techniques (2011): *ISO/IEC 24760-1:2011(E) Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*, http://standards.iso.org/ittf/PubliclyAvailableStandards/c057914_ ISO_IEC_24760-1_2011.zip.

Kamp, Meike und *Weichert, Thilo* (2005): *Scoringsysteme zur Beurteilung der Kreditwürdigkeit - Chancen und Risiken für Verbraucher - Forschungsprojekt im Auftrag des Bundesministeriums für Verbraucherschutz, Ernährung und Landwirtschaft (BMVEL)*, https://www.datenschutzzentrum.de/scoring/2005-studie-scoringsysteme-uld-bmvel.pdf.

Kara Yakup, Boyacioglu Melek Acar and Baykan Ömer Kaan (2011): „Predicting direction of stock price index movement using artificial neural networks and support vector machines: The sample of the Istanbul Stock Exchange", in: *Expert Systems with Applications* 38(5), 5311-5319, http://www.sciencedirect.com/science/article/pii/S0957417410011711.

Kunert, Michael (2013): *Wahltagsbefragung – Exit Poll Grundlage für Prognose und Hochrechnungen*, http://www.infratest-dimap.de/infratest-dimap/methoden/wahltagsbefragung/.

Loemker, Leroy E. (1969): *G. W. Leibniz: Philosophical Papers and Letters*, 2nd ed., Dordrecht: D. Reide.

Ludwig-Mayerhofer, Wolfgang (2005): *Konfidenzintervalle so einfach wie möglich erklärt*, http://www.uni-siegen.de/phil/sozialwissenschaften/soziologie/mitarbeiter/ludwig-mayerhofer/statistik/statistik_downloads/konfidenzintervalle.pdf.

Luhmann, Niklas (1993): *Das Recht der Gesellschaft*, Frankfurt am Main: Suhrkamp Verlag GmbH.

Lutterbeck, Bernd (2013): *WAS WÜRDE WILHELM STEINMÜLLER HEUTE ALS EIN GUTES DATENSCHUTZKONZEPT AKZEPTIEREN? Jochen Schneider und Bernd Lutterbeck spielen Ping Pong*, http://lutterbeck.org/data/uploads/lutterbeck-2013_steinmueller-memorial.pdf.

MacAskill Ewen, Borger Julian, Hopkins Nick, Davies Nick and *Ball James* (2013): *GCHQ taps fibre-optic cables for secret access to world's communications*, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Mantas Carlos J., Puche José M. and Mantas José M. (2006): "Extraction of similarity based fuzzy rules from artificial neural networks", in: *International Journal of Approximate Reasoning*, 43(2), 202-221, http://www.sciencedirect.com/science/article/pii/S0888613X06000338.

Mittal, Sonal (2010): *User Privacy and the Evolution of Third-party Tracking Mechanisms on the World Wide Web*, http://dx.doi.org/10.2139/ssrn.2005252.

Moser, Jeff (2010): *Computing Your Skill*, http://www.moserware.com/2010/03/computing-your-skill.html.

Nissenbaum, Helen (2004): "Privacy as contextual integrity", in: *Washington Law Review* 79(1), 119-158, http://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf

*Parsons, Christopher (*2009): *Deep Packet Inspection in Perspective: Tracing its lineage and surveillance potentials*, http://www.christopher-parsons.com/Academic/WP_Deep_Packet_ Inspection_Parsons_Jan_2009.pdf.

Peter, Saint-Andre (2013): *Protocols*, http://www.webcitation.org/6JqRKj9ji.

Pfitzmann, Andreas und *Hansen, Marit* (2010): *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management* – Version 0.34, TU Dresden, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v 0.34.pdf.

Preis Tobias, Moat Helen Susannah and *Stanley H. Eugene* (2013): „Quantifying Trading Behavior in Financial Markets Using Google Trends", in: *Scientific Reports* 3, Article number 1684, http://www.nature.com/srep/2013/130425/srep01684/full/srep01684.html.

Rojas, Raúl (1996): *Neural Networks - A Systematic Introduction*, Berlin u.a.: Springer, http://page.mi.fu-berlin.de/rojas/neural/neuron.pdf.

Rumpel, Franziska (2009): *Neuromarktforschung. Analyse und Prognose von Markenwahlentscheidungen mittels klassischer und neurowissenschaftlicher Methoden*, http://edoc.bibliothek.uni-halle.de/servlets/MCRFileNodeServlet/HALCoRe_derivate_00003945/Dissertation_Franziska_Rumpel.pdf.

Resnick, Paul (2001): *RFC 2822 Internet Message Format*, http://tools.ietf.org/pdf/rfc2822.pdf.

Resnick, Paul (2008): *RFC 5322 Internet Message Format*, http://tools.ietf.org/pdf/rfc5322.pdf.

Roßnagel, Alexander (2010): „Die "Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, in: *Neue Juristische Wochenschrift* 63(18), 1238-1242, http://beck-online.beck.de/Default.aspx?vpath=bibdata/zeits/njw/2010/cont/njw.2010.1238.1.htm

Rieger, Frank (2010): *Der Mensch wird zum Datensatz*, http://www.faz.net/aktuell/feuilleton/ein-echtzeit-experiment-der-mensch-wird-zum-datensatz-1591336.html.

Schallaböck, Jan und von Damm, Tile (2005): *Digitaler Verbraucherschutz. Verbraucherpolitik im modernen Kommunikations- und Medienzeitalter*, http://www.digitale-chancen.de/transfer/downloads/md780.pdf.

Schneider, Jochen (2011): „Hemmnis für einen modernen Datenschutz: Das Verbotsprinzip", in: *Anwaltsblatt* 61(4), 233-240, http://anwaltsblatt.anwaltverein.de/de/anwaltsblatt/print-archiv?year=2011&file=files/anwaltsblatt.de/Archiv/2011/Jahrgang_2011/Heft-04-2011.pdf.

Schoen, Seth (2009): *New Cookie Technologies: Harder to See and Remove, Widely*, https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide.

Singel, Ryan (2006): *Whistle-Blower Outs NSA Spy Room*, http://archive.wired.com/science/discoveries/news/2006/04/70619.

Socher Richard, Perelygin Alex, Wu Jean Y., Chuang Jason, Manning Christopher D., Ng Andrew Y. and *Potts Christophe*r (2013): *Recursive Deep Models for Semantic Compositionality Over a Sentiment Treebank*, http://nlp.stanford.edu/~socherr/EMNLP2013_RNTN.pdf.

Stockter, Ulrich (2008): *Präventivmedizin und informed consent: Zu den Anforderungen an die informierte Einwilligung in die Teilnahme an Screeningprogrammen*, Berlin u.a.: LIT Verlag.

Tan Jun, Chen Xing-shu, Du Min and *Zhu Kai* (2012): „A novel internet traffic identification approach using wavelet packet decomposition and neural network“, in: *Journal of Central South University*, 19(8), 2218-2230, http://dx.doi.org/10.1007/s11771-012-1266-0.

Typke, Rainer (2009): *Social Lending: Credit Scoring für Normalbürger (mit Open Source-Software)*, http://www.theano.de/uploads/media/LinuxtagSocialLending.pdf.

Wettach, Sven (2006): *Die Geschichte der Umfrageforschung von den 1930er bis in die 1970er Jahre*, http://opus.kobv.de/zlb/volltexte/2007/1098/pdf/Geschichte.pdf.

Whittaker, Zack (2009): *Should universities forget email and use Facebook instead?*, http://www.zdnet.com/blog/igeneration/should-universities-forget-email-and-use-facebook-instead/1198.

Wu Xindong, Kumar Vipin, Quinlan J. Ross, Ghosh Joydeep, Yang Qiang, Motoda Hiroshi, McLachlan Geoffrey J., Ng Angus, Liu Bing, Yu Philip S., Zhou Zhi-Hua, Steinbach Michael, Hand David J. and *Steinberg Dan* (2008): „Top 10 algorithms in data mining“, in: *Knowledge and Information Systems* 14(1), 1-37, http://link.springer.com/article/10.1007%2Fs10115-007-0114-2#.

Unbemerktes Tracking im Internet: Unsere unerwünschte Identität

Dominik Herrmann / Hannes Federrath

1 Einführung

Wie können wir uns im Internet möglichst sicher und komfortabel gegenüber anderen Teilnehmern ausweisen? An Antworten auf diese Frage wird seit vielen Jahren intensiv gearbeitet. Leicht benutzbare und möglichst fälschungssichere Identifizierungsmerkmale erhöhen die Sicherheit und somit das Vertrauen in technische Systeme. Das Streben nach mehr Sicherheit und Vertrauen hat zweifelsfrei seine Berechtigung. Allerdings sollten wir nicht vergessen, dass unsere digitale Identität auch eine Schattenseite hat. Wann immer wir Informations- und Kommunikationssysteme benutzen, hinterlassen wir Spuren. Gerade beim Surfen im Internet oder bei der Benutzung moderner Smartphones entsteht schnell ein beachtlicher „digital footprint“. Abseits der öffentlichen Wahrnehmung hat sich in der Marketingindustrie ein neuer Geschäftszweig etabliert, der sich auf die Auswertung digitaler Spuren spezialisiert hat: Unternehmen wie Turn, Rubicon und Flurry verdienen Geld damit, mittels ausgeklügelter Tracking-Techniken möglichst viele Internet- und Smartphone-Nutzer so genau wie möglich kennenzulernen. Dadurch kommt es zu einer unbemerkten Überwachung der Nutzer, die bislang kaum kontrolliert wird.

In diesem Kapitel werden Tracking-Techniken im Internet beschrieben. Mit den Grundlagen und Motivationen beschäftigen sich die Abschnitte 2 und 3. Anschließend wird in Abschnitt 4 ein Überblick über die gängigen Tracking-Techniken gegeben und herausgearbeitet, welche Schwächen die existierenden Lösungen zum Selbstdatenschutz aufweisen. Bisherige Regulierungsbemühungen können Tracking und Profilbildung ebenfalls nicht eindämmen (s. Abschnitt 5). Abschnitt 6 enthält schließlich einige Denkanstöße und Lösungsansätze.

2 Identitäten im Internet

Es gab eine Zeit, in der man glaubte, sich weitgehend anonym im Internet bewegen zu können. „On the Internet, nobody knows you're a dog", erklärte uns der Cartoonist Peter Steiner augenzwinkernd in einem bekannten Comic, den das US-Magazin *The New Yorker* im Jahr 1993 veröffentlichte. In der Tat konnte man damals die meisten Internetdienste und Webseiten benutzen, ohne eine bzw. seine wahre Identität preiszugeben.

Die dezentrale Struktur des Internets schützt zwar zu einem gewissen Grad die Privatsphäre der Teilnehmer, sie erschwert allerdings auch die Verfolgung missbräuchlicher Aktivitäten. Betrüger können unerkannt Spam-Nachrichten versenden, geheime Zugangsdaten durch Phishing-Angriffe abgreifen oder sich Leistungen unter falscher Identität erschleichen. Dieser Missstand könnte durch eine zuverlässige Identifizierung aller Teilnehmer im Netz behoben werden. So forderte etwa im Jahr 2011 der damalige Innenminister Hans-Peter Friedrich einen Klarnamenzwang für Internet-Nutzer (Lischka 2011). Denkt man diesen Ansatz zu Ende, könnte man zur Überzeugung kommen, dass die Benutzung des Internets im Prinzip ähnlich gefährlich sei wie die Benutzung asphaltierter Verkehrswege; folglich müsste man für jedes einzelne Datenpaket eine Kennzeichenpflicht fordern – eben wie bei Kraftfahrzeugen. Auf internationaler Ebene wäre diese Forderung aber wohl kaum durchsetzbar. Tatsächlich existieren schon heute Authentifizierungsverfahren, etwa auf Basis des neuen Personalausweises, welche die Zurechenbarkeit von Handlungen bei kritischen Anwendungen verbessern können.

Die Zeiten weitgehender Anonymität im Internet sind auch aus einem anderen Grund vorbei: Das Internet dient inzwischen nicht mehr nur der Informationsbeschaffung. Im „Web 2.0" stehen Interaktion und Informationsverbreitung im Vordergrund: Den Nutzern von Facebook, Twitter und Co. bieten sich völlig neue Möglichkeiten zur Selbstinszenierung und Kontaktpflege; die Anhänger der „Quantified Self"-Bewegung erfassen physiologische Daten über ihren Körper und laden sie zur Analyse freiwillig „in die Cloud". Auf Basis der erhobenen Daten erhalten sie dann Vorschläge für die gesündere und effizientere Lebensgestaltung.

Viele Nutzer sind heute dazu bereit, Teile ihrer Identität im Internet offenzulegen. Solche „Teil-Identitäten" enthalten alle freiwillig preisgegebenen Persönlichkeitsmerkmale eines Nutzers (etwa Name, Alter und Geschlecht) sowie zusätzlich die Daten, die der Anbieter bei der Dienstnutzung erhebt, etwa die ausgetauschten Kurznachrichten. Studien haben ge-

zeigt, dass die meisten Nutzer ganz bewusst entscheiden, ob sie Informationen über sich preisgeben, zum Schutz ihrer Privatsphäre unter einem Pseudonym auftreten oder unwahre Daten eingeben (Berendt et al. 2005; Hoffman et al. 1999). Laut der 7. „GVU WWW User Survey" haben etwa 40% der Befragten im Internet schon einmal falsche Angaben gemacht (Hoffman et al. 1999). Nach einer Forsa-Umfrage verwenden deutsche Internetnutzer im Schnitt drei Mail-Adressen (BITKOM 2010). Dadurch können sie ihre Aktivitäten in verschiedenen sozialen Sphären, etwa Beruf, Freizeit und politisches Engagement, voneinander trennen (Nissenbaum 2004).

Zusammenfassend ist festzustellen, dass sich die meisten Nutzer im Internet bewusst eine oder mehrere *erwünschte digitale Identitäten* zulegen. Dadurch üben sie ihr Recht auf informationelle Selbstbestimmung aus, bestimmen also über die Preisgabe und Verwendung ihrer persönlichen Daten. Tatsächlich wird das Recht auf informationelle Selbstbestimmung im Netz jedoch kontinuierlich verletzt. Während der Internetnutzung werden im Hintergrund durch sog. *Tracking* digitale Datenspuren ausgewertet und zu *unerwünschten digitalen Identitäten* miteinander verknüpft. Die weiteren Betrachtungen werden zeigen, dass geltende Datenschutzprinzipien wie Einwilligung, Zweckbestimmung, Kontrolle und Transparenz dabei entweder gar nicht oder nicht angemessen umgesetzt werden. Erschwerend kommt hinzu, dass die Datenerhebung und Analyse sowie die daraus resultierenden Konsequenzen für die betroffenen Nutzer meist überhaupt nicht ersichtlich sind. Daher ist es nicht verwunderlich, dass sich viele Nutzer der Konsequenzen nicht bewusst sind bzw. dass sie ein falsches Verständnis davon haben, welchem Grad an Profilierung sie bereits heute ausgesetzt sind (Ur et al. 2012).

3 Motivation des Trackings: Profilbildung

Praktisch alle kommerziell betriebenen Webseiten kooperieren heute mit Tracking-Anbietern, die das Verhalten von Internetnutzern verfolgen. So stellten etwa Roesner et al. (2012) fest, dass 93% der untersuchten Seiten Third-Party-Cookies (siehe Abschnitt 4.1) setzen. Hoofnagle und Good (2012) kamen in ihrem „Berkeley Web Privacy Census" zu vergleichbaren Ergebnissen (s.a. Hoofnagle et al. 2012).

Tracking-Anbieter sind ein integraler Bestandteil des komplexen Online-Marketing-Systems. Aus Sicht der Anbieter geht es im Wesentlichen

darum, möglichst wirkungsvoll Werbung zu schalten bzw. Produkte zu vermarkten. Hintergrundinformationen zum Markt für Online-Werbung finden sich beispielsweise bei Kleindl und Theobald (1999) und bei Turow (2011).

3.1 Motivation

Die meisten Internetnutzer sind bisher nicht dazu bereit, für den Abruf von Informationen bzw. für die Benutzung von Onlinediensten zu bezahlen. Zwar werden mehr und mehr Versuche unternommen, dies zu ändern, etwa bei den Online-Angeboten von bild.de, wo ganze Inhaltsbereiche kostenpflichtig sind, oder nytimes.com, wo derzeit nur noch zehn Artikel pro Monat kostenlos sind. Wegen der bisher fehlenden Zahlungsbereitschaft für Inhalte vermarkten die Anbieter aber überwiegend Werbeflächen auf ihren Webseiten. Vereinfacht gesagt stellen sich bei der Einblendung von Werbung zwei Fragen:

1. Zu welchen Konditionen erfolgt die Einblendung?
2. Welche Werbung soll eingeblendet werden?

Bei der Beantwortung dieser Fragen spielen Tracking-Dienste eine zentrale Rolle. Der Preis, den eine Webseite vom Werbetreibenden verlangen kann, hängt von den aus dem Zeitungsverlagswesen bekannten Mediadaten ab, die u.a. angeben, welche Reichweite („unique visitors“) eine Webseite aufweist. Um diese Informationen zu erheben, wird jeder Besucher mit einem Tracking-Cookie (s. Abschnitt 4.1) markiert. Grundsätzlich können die Webseitenbetreiber diese Form des Trackings selbst durchführen. Üblicherweise wird die Reichweitenmessung jedoch an externe Dienstleister ausgelagert, etwa an den von der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern (IVW) betriebenen Dienst INFOonline (http://www.infoonline.de).

Die Preisgestaltung hängt allerdings nicht nur von der Reichweite einer Webseite ab, sondern auch vom Erfolg einer Werbemaßnahme. Das bloße Einblenden von Werbebannern wird mit äußerst geringen Beträgen vergütet. Wesentlich höhere Beträge werden bezahlt, wenn ein Nutzer ein Werbebanner anklickt bzw. das beworbene Produkt kauft oder eine entsprechende Buchung abschließt („conversions“). Für dieses Erfolgsbeteiligungsmodell ist eine seitenübergreifende Verfolgung der Nutzer erforder-

lich. Diese Aufgabe übernehmen die sog. *Werbenetze*, die im Internet als Vermittler zwischen Werbetreibenden und Webseitenbetreibern fungieren.

Um möglichst viele Conversions zu erzielen, muss die Werbung die gewünschte Zielgruppe erreichen („targeting"). Die Betreiber der Werbenetze entscheiden manuell oder vollautomatisch, welche Anzeigen auf welcher Webseite eingeblendet werden. Eine einfache, aus den Printmedien bekannte Strategie besteht darin, das Targeting anhand der Zielgruppe durchzuführen, an die sich eine Webseite richtet („demographic targeting"). Eine genauere Abstimmung auf die Interessen der Nutzer lässt sich erreichen, indem der Inhalt jeder einzelnen Unterseite analysiert wird, um dort jeweils thematisch passende Anzeigen einzublenden („contextual targeting"). Bei beiden Ansätzen sehen alle Besucher einer Webseite im Laufe der Zeit dieselben Anzeigen.

Beim *verhaltensbasierten Targeting* („behavioral targeting") werden die eingeblendeten Anzeigen hingegen individuell auf jeden einzelnen Nutzer abgestimmt (Yan et al. 2011). Da die Werbenetze mit einer Vielzahl von Webseiten kooperieren, können sie nachvollziehen, welche Webseiten ein Nutzer im Zeitverlauf besucht. Mit diesem Wissen kann ein Werbenetz Anzeigen auswählen, die unmittelbar auf den aktuellen Bedarf eines Nutzers zugeschnitten sind. So wird einem Nutzer, der gerade einen Flug gebucht hat, Werbung von Hotel-Buchungsportalen und Autovermietungen angezeigt. Eine Variante davon ist das *Re-Targeting*: Hat ein Nutzer sich in einem Onlineshop umgesehen, jedoch nichts gekauft, dann verfolgen ihn Anzeigen genau dieses Onlineshops auch auf anderen Webseiten, um ihn doch noch zum Abschluss des Geschäfts zu bewegen.

Sein größtes Potential entfaltet das verhaltensbasierte Targeting jedoch erst, wenn die dabei erhobenen Daten über einen längeren Zeitraum analysiert werden, um daraus ein Nutzerprofil zu erstellen. Die besuchten Seiten geben Aufschluss über Persönlichkeitsmerkmale wie Geschlecht und Alter sowie über das Umfeld eines Menschen, etwa seinen Familienstand und seine finanzielle Situation. Auch die Interessen und Neigungen eines Menschen, etwa die politische und sexuelle Orientierung, sowie die Intensität, mit denen er diesen nachgeht, können häufig mit überraschend hoher Genauigkeit aus dem Online-Verhalten abgeleitet werden.

Die erhobenen Nutzerprofile spielen nicht nur beim Targeting eine Rolle; sie bilden auch die Grundlage für die Preisgestaltung der Anzeigen. Beim sog. *Real-Time-Bidding* wird die Einblendung jeder einzelnen Anzeige versteigert. Besucht ein Nutzer eine Webseite, wird sein Nutzungsprofil auf einem Marktplatz mehreren Werbetreibenden zur Verfügung ge-

stellt. Innerhalb von Millisekunden geben diese mithilfe von Software-Agenten ein Gebot ab, das ihre Zahlungsbereitschaft für die Einblendung bzw. für die Conversion-Erfolgsprämie enthält (Singer 2012).

Die Marketingindustrie ist vom Erfolg des verhaltensbasierten Targetings überzeugt. Eine von der Industrie finanzierte Studie (Beales 2009) nennt konkrete Zahlen. Demnach verdoppele sich die Anzahl der Conversions durch das verhaltensbasierte Targeting im Vergleich zu wahllos ausgesuchten Anzeigen („run on network advertising"). Aus Sicht der Industrie profitieren davon auch die Internetsurfer: Sie sähen schließlich weniger irrelevante Werbung, also störende Anzeigen, die gar nicht zu ihren Interessen passten.

3.2 Risiken der Profilbildung

Die Nutzer sehen das anders: Die Mehrheit ist nicht damit einverstanden, dass anhand des Surfverhaltens Persönlichkeitsprofile erzeugt werden, um die eingeblendeten Anzeigen darauf abzustimmen (Mayer und Mitchell 2012). Wie die im Folgenden skizzierten Risiken der Profilbildung zeigen, sind diese Vorbehalte durchaus berechtigt.

Die verhaltensbasierte Auswahl der Anzeigen kann zum einen gezielt die Wahrnehmung manipulieren: Den Nutzern wird nur noch der Teil des gesamten verfügbaren Marken- und Produktangebots präsentiert, der vom Werbenetz automatisch ausgewählt wird. Die Auswirkungen beschränken sich zudem nicht auf die eingeblendeten Anzeigen. Die Persönlichkeitsprofile werden auch zur Personalisierung von Informationsangeboten eingesetzt: Sie beeinflussen schon heute die Auswahl der Suchergebnisse, die Google seinen Nutzern anzeigt, und die Neuigkeiten aus dem Freundeskreis, die in der eigenen Facebook-Timeline erscheinen. Facebook hat 2012 hierzu selbst ein umstrittenes Experiment durchgeführt und herausgefunden, dass der Anteil positiver bzw. negativer Facebook-Einträge in der Timeline eines Nutzers einen Einfluss darauf hat, ob er selbst eher positive bzw. negative Einträge verfasst (Kramera et al. 2013).

Zum einen können Werbenetze und Inhaltsanbieter also unbemerkt die Stimmung eines Nutzers manipulieren. Zum anderen kann sich eine „Filter Bubble" bilden. Bei weitgehender Personalisierung würde man im Extremfall nur noch die Informationen zu Gesicht bekommen, die zur eigenen Persönlichkeit passen. All das Neue und gerade deswegen Interessante würde hingegen ausgefiltert. In der Folge könnte sich unsere Persönlich-

keit womöglich weniger frei entfalten und weiterentwickeln (Pariser 2011).

Darüber hinaus können die Nutzungsprofile zur Diskriminierung eingesetzt werden, etwa indem der Preis eines Produktes an die vermutete Zahlungsbereitschaft eines Nutzers angepasst wird. Eine subtile Form von Preisdiskriminierung wurde beim Hotel-Buchungsportal Orbitz nachgewiesen. Dort wurde die Reihenfolge der gefundenen Hotels verändert (Mattioli 2012). Da Orbitz Apple-Nutzern eine höhere Zahlungsbereitschaft unterstellte, sortierte das Unternehmen bei diesen Nutzern die hochwertigen Hotels weiter nach oben, um sie zum Abschluss einer teureren Buchung zu verleiten. Die Diskriminierung kann allerdings auch schwerere Folgen haben, indem etwa einzelnen Nutzern der Zugang zu bestimmten Produkten und Angeboten verwehrt wird. So könnte etwa der Abschluss einer Risikolebensversicherung verweigert werden, weil sich ein Nutzer zuvor ausgiebig über eine bestimmte Krankheit informiert hat.

4 Tracking-Techniken und Schutzmöglichkeiten

Weil die Marketingindustrie von der Effektivität des verhaltensbasierten Trackings überzeugt ist, betreibt sie einen hohen Aufwand, um die Aktivitäten von Internetnutzern möglichst genau zu verfolgen. Datenschützer und Browser-Hersteller arbeiten hingegen an Techniken, mit denen die Privatsphäre der Nutzer geschützt werden kann.

Die verwendeten Tracking-Techniken lassen sich in drei Kategorien einteilen. Am bekanntesten sind Tracking-Techniken, die einen Nutzer bzw. sein Endgerät *gezielt mit einer Tracking-ID markieren*. Dabei handelt es sich meist um große Zufallszahlen, sog. „Globally Unique IDs“ (abgekürzt GUIDs). Die zweite Kategorie umfasst Techniken, die technisch bedingte *Eigenschaften der verwendeten Endgeräte auslesen*, um die Geräte verschiedener Nutzer voneinander zu unterscheiden (aktives Fingerprinting). In die dritte Kategorie fallen schließlich *passive Tracking-Techniken*, bei denen lediglich der Datenverkehr beobachtet wird.

Die nachfolgend beschriebenen Tracking-Techniken dienen zunächst nur der Verkettung von Nutzeraktivitäten. Aus Sicht der Marketingindustrie besteht der Wunsch, das Nutzungs- oder Konsumprofil eines Kunden möglichst genau zu kennen. Um effektiv Marketing betreiben zu können, ist die Identität eines Kunden eigentlich zweitrangig – Hauptsache, die Bedürfnisse und Interessen eines konkreten Kunden werden genau getroffen.

Da allerdings fast immer im Online-Kaufprozess an irgendeinem Punkt der Kommunikation nach der Identität des Kunden gefragt werden muss, etwa eine Lieferanschrift oder um Zahlungsdaten zu überprüfen, sind die Profile keineswegs nur pseudonym. Zudem sind die Anbieter von Online-Shops und von Online-Marketing längst eng miteinander verflochten. Wenn also der Online-Shop die Identität zu einem Kunden kennt, ist es nur eine Frage der Zeit, bis die Marketingindustrie einem Profil auch die Identität zuordnen kann. Omnipräsente Online-Anbieter wie Google (gmail) kennen ohnehin die Identitäten ihrer Kunden *und* betreiben Dienste zum Online-Marketing (AdWords), können also unmittelbar identifizierbare Profile anlegen.

4.1 Markierung mit Tracking-IDs

Zum Tracking von Nutzern werden im Internet heute meistens HTTP-Cookies eingesetzt bzw. zweckentfremdet. Ursprünglich sollten HTTP-Cookies nämlich lediglich die Programmierung von interaktiven Webseiten erleichtern. Viele Webseiten sind darauf angewiesen, die Eingaben eines Nutzers über mehrere Anfragen hinweg verketten zu können, was ohne HTTP-Cookies nicht zuverlässig gelingt.

Zur Verkettung ordnet der Webserver jedem Nutzer eine eindeutige Kennung (Session-ID) zu. Diese wird im HTTP-Header-Feld „Set-Cookie“ an den Browser übermittelt. Der Browser speichert die erhaltenen Cookies in einer Datenbank auf dem Rechner des Nutzers. Ist in dieser Datenbank für den gerade zu kontaktierenden Webserver bereits ein Cookie vorhanden, übermittelt der Browser es automatisch im HTTP-Header-Feld „Cookie“ an den Server. Der Webserver liest die Session-ID dann wieder aus dem Cookie aus und ruft die relevanten Zustandsdaten aus seiner Session-Datenbank ab.

Ein einzelner Webserver kann anhand „seiner“ Cookies nicht ohne weiteres herausfinden, welche anderen Webseiten ein Nutzer besucht hat. Werbenetze können die Aktivitäten eines Nutzers allerdings trotzdem über Webseitengrenzen hinweg nachvollziehen. Dabei wird ausgenutzt, dass nicht nur der Webserver, von dem die eigentliche Webseite heruntergeladen wird, Cookies setzen kann (sog. First-Party-Cookies), sondern auch alle anderen Webserver, die beim Abruf einer Webseite kontaktiert werden, um z.B. Bilder nachzuladen (sog. *Third-Party-Cookies*). Webseiten, die an einem Werbenetz teilnehmen, binden die Werbebanner so ein, dass

sie direkt von den Webservern des Werbenetzes heruntergeladen werden. Beim Abruf erfährt das Werbenetz zum einen die Adresse der aktuell besuchten Webseite, da diese im sog. Referrer-HTTP-Header und ggf. zusätzlich explizit als URL-Parameter übermittelt wird. Zum anderen kann das Werbenetz einen Nutzer anhand seiner *Tracking-ID*, einer langlebigen Session-ID, die in einem Third-Party-Cookie hinterlegt wird, wiedererkennen.

Viele Publikumsmedien haben in der Vergangenheit über Tracking-Techniken berichtet und die Nutzer dafür sensibilisiert. Beachtenswert sind beispielsweise die Rubriken „What They Know" des Wall Street Journals und „Tracking the Trackers" im Guardian (Angwin 2010; Geary 2012). In Deutschland berichtete u.a. Der Spiegel (Schmundt 2012). Die Hersteller der weitverbreiteten Browser (Firefox, Chrome, Safari und Internet Explorer) haben daher verschiedene Funktionen in ihre Software integriert, mit denen Nutzer die Cookie-Verwaltung beeinflussen können.

Eine Möglichkeit zur Eindämmung des Trackings mittels Cookies besteht darin, die Cookies zwar anzunehmen, allerdings regelmäßig zu löschen. Alle gängigen Browser können die Cookies auf Knopfdruck bzw. beim Beenden des Browsers entfernen. Viele Nutzer (zwischen 20 und 70%) machen von diesen Möglichkeiten Gebrauch (Lavin 2006; McDonald und Cranor 2010). Das regelmäßige Löschen der Cookies führt allerdings zu einem gewissen Komfort-Verlust. Man muss sich danach bei allen Webseiten wieder neu einloggen und Hinweise und Warnungen wegklicken, die man in früheren Sitzungen bereits zur Kenntnis genommen hat. Hinzu kommt, dass das Löschen der Cookies das Tracking ohnehin nicht wirkungsvoll verhindert, wie sich im weiteren Verlauf zeigen wird.

Alle Browser können auch so eingestellt werden, dass sie überhaupt keine Cookies akzeptieren – das Tracking mittels Cookies ist dann zwar nicht mehr möglich, allerdings funktionieren auch alle Webseiten, die auf Sitzungen angewiesen sind, nicht mehr wie erwartet. Sinnvoller erscheint es, die Cookie-Sperre ausschließlich auf die Third-Party-Cookies zu beschränken; was beim Safari-Browser der Voreinstellung entspricht. Diese Maßnahme ist jedoch umstritten. Als die Mozilla Foundation im Jahr 2013 ankündigte, in Zukunft Third-Party-Cookies in der Standardkonfiguration des Firefox-Browsers automatisch ablehnen zu wollen (Mayer 2013), trugen die Betreiber zahlreicher Webseiten Bedenken vor: Angeblich gäbe es eine Vielzahl legitimer Webseiten, etwa Single-Sign-On-Dienste, die auf Third-Party-Cookies angewiesen seien (Temple 2014). Wohl auch auf Druck der Marketingindustrie gab Mozilla seine Pläne wieder auf. Statt-

dessen wolle man in Zukunft eine Blockliste mit unerwünschten Tracking-Domains in den Browser integrieren, ein Ansatz, der bereits von den Browser-Erweiterungen „Ghostery“ und „Adblock Plus“ bekannt ist.

Das Blockieren von Third-Party-Cookies reicht inzwischen allerdings ohnehin nicht mehr aus. Die Werbenetze gehen dazu über, ihre Tracking-IDs in First-Party-Cookies zu hinterlegen. Zum seitenübergreifenden Tracking müssen die teilnehmenden Webseiten dann nur die Tracking-IDs untereinander austauschen. In welchem Umfang ein solches *Cookie-Syncing* durchgeführt wird, lässt sich nicht genau feststellen. Eine aktuelle Studie kommt allerdings zu dem Ergebnis, dass zahlreiche Werbenetze bereits die erforderlichen technischen Voraussetzungen geschaffen haben (Acar et al. 2014).

Soziale Netzwerke wie Facebook können Third-Party-Cookie-Sperren auch ohne Cookie-Syncing aushebeln. Einige Browser lassen es nämlich zu, ein Cookie, das im First-Party-Kontext, also z.B. beim Besuch des Sozialen Netzwerks, gesetzt wurde, im Third-Party-Kontext wieder auszulesen. Wird auf einer Webseite ein „Like“-Button eingebettet, kann Facebook also die zuvor gesetzte Tracking-ID auslesen und den Besucher daran wiedererkennen. Damit nicht genug: Google integrierte in den Code zum Einbetten von „Google Plus“-Buttons zusätzliche Mechanismen, um gezielt die strengen Cookie-Sperren der Browser Safari und Internet Explorer zu überlisten (Bager 2012).

Neben HTTP-Cookies verwenden Tracking-Dienste auch noch andere Techniken, um Nutzer gezielt zu markieren. Eine Vorreiterrolle nehmen dabei die sog. Flash-Cookies (sog. „Local Shared Objects“) ein. Dabei handelt es sich um einen Datenspeicher im Browser, der über das Flash-Browser-Plug-in angesprochen wird (Soltani et al. 2009). Flash-Cookies zeichneten sich lange Zeit dadurch aus, dass sie nicht entfernt wurden, wenn ein Nutzer die HTTP-Cookies im Browser löschte. Die Hersteller haben erst Abhilfe geschaffen, als öffentlich bekannt wurde, dass Werbenetze Flash-Cookies benutzen, um ihre Tracking-IDs nach dem Löschen der HTTP-Cookies zu rekonstruieren. Für solche robusten Markierungen haben sich die Begriffe „Supercookie“ bzw. „Evercookie“ etabliert.

Mit der Einführung von HTML5 kommt ein weiterer Datenspeicher hinzu („HTML5 Local Storage“). Dieser ist eigentlich dafür vorgesehen, die Ladezeiten zu verkürzen und temporäre Verbindungsunterbrechungen zu überbrücken. HTML5-Storage sowie alternative Ansätze wie IndexedDB werden inzwischen allerdings auch zum Ablegen von Tracking-IDs benutzt (Acar et al. 2014; Ayenson et al. 2011).

Sogar im Browser-Cache hinterlegen die Werbenetze ihre Tracking-IDs (sog. *Cache-Cookies*). Dazu instruieren sie den Browser, eine JavaScript-Datei herunterzuladen, in der die Tracking-ID einer globalen Variable zugewiesen wird. Dieser Datei weist der Webserver mit dem Expires-HTTP-Header ein Cache-Ablaufdatum zu, das in ferner Zukunft liegt, sodass der Browser sie für einen langen Zeitraum im Cache zwischenspeichert. Bei späteren Aktivitäten veranlasst das Werbenetz den Browser, die hinterlegte Tracking-ID direkt aus dem Cache auszulesen und sie an den Webserver zurückzusenden. Eine andere Variante von Cache-Cookies funktioniert auch ohne JavaScript; dabei werden die HTTP-Header „ETag“ und „Last-Modified“ zum Speichern der Tracking-ID missbraucht (Ayenson et al. 2011; Juels et al. 2006). Um das Tracking zu unterbinden, muss somit auch der Browser-Cache regelmäßig geleert bzw. vollständig deaktiviert werden.

Zusätzlich werden die Tracking-IDs auch in *flüchtigen* Datenspeichern abgelegt – was durchaus Sinn macht. Ein Beispiel hierfür ist die JavaScript-Eigenschaft „window.name“, in der für jedes Browser-Fenster bzw. jeden Tab ein interner Bezeichner hinterlegt werden kann. Die Folge: Solange das Fenster nicht geschlossen wird, kann die Tracking-ID dort ausgelesen werden, also selbst dann, wenn ein Nutzer Cookies, lokale Datenspeicher und Browser-Cache gelöscht hat. Zum Schutz vor Tracking müssen also zusätzlich alle Browser-Fenster geschlossen werden.

Neben den hier genannten Beispielen gibt es zahlreiche weitere Techniken, die von Werbenetzen zum Abspeichern eines Supercookies eingesetzt werden. Eine Aufstellung der bekanntesten Vertreter findet sich bei Mayer und Mitchell (2012). Zusammenfassend lässt sich feststellen, dass Online-Marketingfirmen grundsätzlich sinnvolle Browser-Funktionen zum Tracking missbrauchen. Zum einen ist es für die Nutzer dadurch kaum möglich, alle Markierungen zuverlässig zu entfernen. Zum anderen stehen die Nutzer dabei vor einem Zielkonflikt: Um sich gegen die Überwachung ihrer Aktivitäten zu wehren, müssen sie eigentlich wünschenswerte Funktionen des Browsers deaktivieren.

4.2 Aktives Fingerprinting

Selbst mit Supercookies ist eine zuverlässige Markierung von technisch versierten bzw. sehr sensiblen Nutzern nicht möglich. Die Werbenetze setzen daher zusätzlich Techniken ein, mit denen sich auch diejenigen Nutzer

wiedererkennen lassen, die Cookies und Cache regelmäßig löschen. Hier gibt es zwei unterschiedliche Ansätze:

1. Das Auslesen implizit vorhandener charakteristischer Eigenschaften von Endgeräten.
2. Das Auslesen von eindeutigen Geräte-Kennungen, die explizit zur Wiedererkennung von Endgeräten vorgesehen sind.

Den ersten Ansatz bezeichnet man als *Browser-* bzw. *Device-Fingerprinting*. Wegweisend war hier insbesondere die Panopticlick-Studie der Electronic Frontier Foundation (Eckersley 2010). Auf der Webseite https://panopticlick.eff.org/ kann man überprüfen, ob der eigene Browser einen einzigartigen Fingerabdruck aufweist, der zum Tracking ausgelesen werden kann. Inzwischen sind mehr als vier Millionen Browser-Fingerprints ausgewertet worden; der Großteil davon erwies sich als einzigartig. Dieses Ergebnis ist darauf zurückzuführen, dass die meisten Nutzer ihr System im Laufe der Zeit nach ihren Wünschen angepasst haben. Zur Bestimmung des Fingerabdrucks werden mittels JavaScript und Flash möglichst viele Systemeinstellungen und Anpassungen ausgelesen, etwa die bevorzugte Sprache, die eingestellte Zeitzone und die Bildschirmauflösung. Diese Informationen werden vom Browser eigentlich für einen sinnvollen Zweck preisgegeben: Webseiten können sich dadurch besser auf den Benutzer und seine Umgebung einstellen.

Besonders charakteristische Merkmale lassen sich aus der Liste der installierten Browser-Plug-ins sowie den im System installierten Schriftarten generieren. Die installierten Schriftarten lassen sich allerdings nicht ohne weiteres auflisten. Die Tracking-Dienste bedienen sich daher eines Seitenkanals (Acar et al. 2013; Nikiforakis et al. 2013). Dabei wird ausgenutzt, dass sich die Zeichen verschiedener Schriftarten hinsichtlich ihrer Abmessungen unterscheiden. Die Tracking-Dienste verfügen über eine Datenbank, welche die Abmessungen einer bestimmten Buchstabenfolge für eine Vielzahl von Schriftarten enthält. Zum Fingerprinting wird der Browser mittels JavaScript angewiesen, die Buchstabenfolge nach und nach mit allen Schriftarten aus der Datenbank darzustellen. Anhand der Abmessungen der Buchstabenfolge wird dann überprüft, ob die jeweilige Schriftart installiert ist oder nicht.

Ähnlich wird beim sog. *Canvas-Fingerprinting* vorgegangen, das inzwischen ebenfalls in der Praxis verbreitet ist (Acar et al. 2014). Auch bei dieser Technik werden Unterschiede bei der Darstellung von Text ausgenutzt. Mowery und Shacham (2012) fanden heraus, dass in einer HTML5-

Canvas-Umgebung ein und derselbe Text auf verschiedenen Systemen auch dann unterschiedlich dargestellt wird, wenn dieselbe Schriftart zum Einsatz kommt. Dieses Phänomen ist auf das Weichzeichnen der Buchstabenränder (Antialiasing) zurückzuführen, das vom Grafikchip bzw. seinem Treiber durchgeführt wird und auf unterschiedliche Weise implementiert werden kann. Hardware-Unterschiede werden auch beim Device-Fingerprinting-Verfahren von Mowery et al. (2011) ausgenutzt: Anhand der Laufzeitunterschiede einiger JavaScript-Funktionen kann man auf die CPU-Architektur schließen bzw. die ungefähre CPU-Taktrate bestimmen.

Mit den vorgestellten Fingerprinting-Verfahren lassen sich vor allem Desktop-PCs von Privatnutzern wiedererkennen. Die Verfahren versagen jedoch bei völlig baugleichen bzw. identisch konfigurierten Endgeräten, die z.B. in Unternehmen eingesetzt werden, sowie bei Tablets und Smartphones. Zum einen ist hier die Anzahl der Baureihen bzw. Varianten vergleichsweise klein, zum anderen können die Nutzer diese Geräte nur eingeschränkt anpassen und personalisieren. Für die auf Smartphones vorinstallierten Browser Apple Safari und Google Chrome gibt es daher (noch) keine wirkungsvollen Device-Fingerprinting-Techniken, mit denen einzelne Endgeräte wiedererkannt werden können.

Anders verhält es sich hingegen mit *Apps*, also den Anwendungen, die auf mobilen Endgeräten installiert werden. Diese verfügen im Vergleich zu einer Webseite, die im Browser dargestellt wird, über wesentlich umfangreichere Berechtigungen. Wie Kurtz (2014) zeigt, kann jede iOS-App eine Liste aller installierten Anwendungen anfertigen. Da die installierten Apps meist persönliche Vorlieben widerspiegeln, dürften sich viele Menschen dadurch ziemlich eindeutig identifizieren lassen. Zusätzlich können Apps die Werte zahlreicher Systemeinstellungen auslesen, etwa ob neben der grafischen Akku-Ladestand-Anzeige zusätzlich ein Prozentwert stehen soll. In einer Feldstudie hat Becker (2014) gezeigt, dass Apps anhand der auslesbaren Informationen weitgehend eindeutige Device-Fingerprints erstellen können (Oestreich 2014).

Neben diesen Device-Fingerprinting-Techniken gibt es bei den gängigen Smartphones allerdings noch eine viel zuverlässigere Möglichkeit, einzelne Endgeräte wiederzuerkennen. Jedes mobile Endgerät verfügt bereits ab Werk über eine GUID (unter iOS die UDID, unter Android die sog. „Android ID“). Abgesehen davon existieren verschiedene Hardware-Adressen, etwa die MAC-Adresse des WLAN- oder Bluetooth-Moduls, die GSM-Gerätekennung (IMEI) sowie die IMSI-Kennung und die Rufnummer der eingelegten SIM-Karte. Da sich diese Merkmale – vor allem

miteinander kombiniert – sehr gut zur zuverlässigen Wiedererkennung eignen, werden sie von vielen Entwicklern verwendet, meist ohne die Nutzer darüber zu informieren. Auch Werbenetze greifen auf die o.g. GUIDs und Adressen zurück, um verhaltensbasiertes Targeting in werbefinanzierten Apps zu betreiben.

Inzwischen sind Apple und Google bestrebt, den Zugriff auf die System-IDs und die Geräte-Adressen zu unterbinden, um die Privatsphäre ihrer Kunden besser zu schützen. Um den Nutzern mehr Kontrolle zu geben, werden den Entwicklern spezielle GUIDs zur Verfügung gestellt. Seit iOS 6 gibt es den „Identifier for Advertisers“ (IDFA) zum App-übergreifenden Tracking bzw. verhaltensbasierten Targeting von Werbung (Apple 2014). Unter Android existiert mit der „Advertising ID“ ein vergleichbarer Mechanismus (Google 2014). Die Nutzer können diese IDs in den Systemeinstellungen jederzeit auf einen neuen zufälligen Wert setzen, um die Verkettung ihrer Aktivitäten zu unterbrechen. Darüber hinaus gibt es eine Systemeinstellung, mit der Apps angewiesen werden können, auf das verhaltensbasierte Targeting zu verzichten. Wie beim Do-not-Track-Ansatz (s. Abschnitt 5) lässt sich jedoch nicht kontrollieren, ob dieser Wunsch respektiert wird: Die o.g. GUIDs können die Apps nämlich trotzdem auslesen und zur Wiedererkennung verwenden.

Die oben genannten Ansätze der Smartphone-Hersteller sind grundsätzlich zu begrüßen; zuverlässigen Schutz vor Tracking bieten sie jedoch nicht. Die Hersteller sollten die Nutzer z.B. nach der Installation oder bei einem Software-Update nach ihren Tracking-Präferenzen fragen. Auf Wunsch des Nutzers sollte das Betriebssystem dann das Auslesen der GUIDs völlig verhindern oder die GUIDs zumindest regelmäßig, etwa täglich, erneuern.

Wesentlich schwieriger gestaltet sich hingegen der Schutz vor den o.g. Fingerprinting-Techniken. Das Deaktivieren von JavaScript verhindert zwar zuverlässig den Zugriff auf charakteristische Merkmale, geht jedoch mit erheblichen Komforteinbußen einher. Stattdessen könnte man die Endgeräte mit einer Fingerprinting-Erkennung (vgl. Acar et al.2013) ausstatten, die beim Aufruf verdächtiger Funktionen die Ausführung unterbricht. Dieser Ansatz unterliegt jedoch grundsätzlichen Einschränkungen, die bereits von Intrusion-Detection-Systemen und Virenscannern bekannt sind: Weder Fehler erster Art (erfolgreiches Fingerprinting, das nicht verhindert wurde) noch Fehler zweiter Art (fälschlicherweise erkanntes Fingerprinting) lassen sich zuverlässig vermeiden.

4.3 Tracking durch passives Beobachten

Im vorigen Abschnitt wurden Techniken vorgestellt, mit denen Nutzer durch aktives Auslesen charakteristischer Eigenschaften ihrer Endgeräte wiedererkannt werden können. Es gibt jedoch auch passive Techniken zur Profilbildung, die keinen Code auf dem Endgerät des Nutzers ausführen und daher dort nicht erkennbar sind.

Kohno et al. (2005) zeigten, dass ein Kommunikationspartner oder ein Außenstehender ein bestimmtes Endgerät *anhand des Taktversatzes* („clock skew“) seiner internen Uhr wiedererkennen kann. Dazu muss er lediglich die Zeitstempel im TCP-Timestamp-Feld analysieren. Da jede Uhr aufgrund von Fertigungstoleranzen eine einzigartige Taktfrequenz hat, also etwas zu schnell oder zu langsam läuft, bildet sich im Laufe der Zeit ein charakteristischer Gangunterschied heraus, der sich zur Langzeit-Wiedererkennung eignet. Bislang können nur versierte Nutzer die Übermittlung der TCP-Timestamps deaktivieren.

Werbenetze können bis zu 77% des Nutzungsverhaltens beobachten (Acar et al. 2014; Abdelberi et al.2012). Dies versetzt sie in die Lage, eine rein *verhaltensbasierte Verkettung* von Sitzungen durchzuführen. Dabei wird ausgenutzt, dass die meisten Menschen charakteristische Interessen und Vorlieben haben: Sie besuchen also regelmäßig ihre Lieblingsseiten. Werbenetze können maschinelle Lernverfahren einsetzen, um solche Verhaltensmuster zu extrahieren und zu einem späteren Zeitpunkt einen Nutzer daran wiederzuerkennen. In Herrmann et al. (2010; 2013) werden geeignete Verfahren vorgestellt. Bei einer Studie mit 3.600 Nutzern ließen sich allein anhand der aufgelösten Domainnamen 86% der Sitzungen korrekt miteinander verketten.

Wie weitere Untersuchungen belegen, lässt sich die Verkettung selbst durch das Absenden zusätzlicher zufälliger Anfragen nicht völlig verhindern, sondern nur erschweren. Als wenig praktikabel, aber durchaus wirksam erweisen sich hingegen besonders kurzlebige dynamische IP-Adressen. Die Nutzer müssten dazu alle paar Minuten ihre IP-Adresse ändern und jedes Mal sämtliche Tracking-IDs löschen bzw. wechseln (vgl. Lindqvist und Tapio 2008). Allerdings fehlen bisher praktisch verfügbare Lösungen, die derartige Datenschutztechniken implementieren. Mit der Einführung von IPv 6 wäre zumindest der Vorrat an IP-Adressen groß genug, um solche Verfahren zu implementieren (Herrmann et al. 2012).

5 Regulierungsbestrebungen

Technische Mechanismen allein können die Profilierung von Nutzern nicht zuverlässig verhindern. Sowohl in Europa als auch in den Vereinigten Staaten wird daher diskutiert, ob staatliche Regulierung eine Lösung sein könnte.

In den USA verfolgt man bislang den Ansatz der Selbstregulierung. Das daraus hervorgegangene *Do-not-Track-Konzept* (DNT-Konzept) sieht vor, dass sich die Marketingindustrie dazu verpflichtet, die Datenschutzpräferenzen der Nutzer zu respektieren und ggf. auf verhaltensbasiertes Targeting zu verzichten. Ein entsprechend konfigurierter Browser übermittelt in seinen Anfragen einen HTTP-Header („DNT:1“). Allerdings können die Nutzer nicht überprüfen, ob sich die Tracking-Dienste an ihren Wunsch halten – schließlich setzen sie weiterhin Cookies mit Tracking-IDs und versprechen lediglich, diese nicht zum Targeting heranzuziehen.

Die meisten Browser können inzwischen so konfiguriert werden, dass sie auf Wunsch des Nutzers einen DNT-Header senden. Obwohl diese Funktion bislang kaum aktiv beworben wurde, hatten im Jahr 2013 schon mehr als 10% der Firefox-Nutzer den DNT-Header aktiviert (siehe https://dnt-dashboard.mozilla.org/). Unter den primär studentischen Besuchern der Webseite des Arbeitsbereichs „Sicherheit in verteilten Systemen“ der Universität Hamburg ist der Anteil sogar noch höher: Inzwischen ist dort der DNT-Header bei über 30% der HTTP-Anfragen gesetzt. Gerade wegen seiner Einfachheit ist das DNT-Konzept so benutzerfreundlich. Insofern ist es zu bedauern, dass die Standardisierung des World Wide Web Consortiums (W3C) ins Stocken geraten ist: Die Vertreter der Marketingindustrie haben die „Tracking-Protection“-Arbeitsgruppe des W3C wieder verlassen (Clarke 2013). Einige Anbieter, darunter Google, Facebook und Yahoo, haben zudem angekündigt, den DNT-Header zu ignorieren (Ackermann 2013; Dwoskin 2014).

Die EU setzt anstelle der Selbstregulierung hingegen auf gesetzliche Vorschriften. Die als „Cookie-Richtlinie“ bekannt gewordenen Richtlinie 2009/136/EG verfolgt einen Opt-in-Ansatz: Sie verlangt vor dem Setzen von Cookies grundsätzlich eine Einwilligung des Nutzers (Neufassung von Art. 5 Abs. 3 der Richtlinie 2002/58/EG). In Erwägungsgrund 66 der Richtlinie wird dieses Prinzip allerdings wieder aufgeweicht: Zum einen dürfen Cookies, die für einen vom Nutzer ausdrücklich angeforderten Dienst unverzichtbar sind, ohne vorheriges Einverständnis gesetzt werden, zum anderen wird angedeutet, dass die Einwilligung auch implizit durch

eine entsprechende Browserkonfiguration erfolgen kann. Ob die Konfiguration „alle Cookies akzeptieren" bereits eine solche Einwilligung darstellt, ist umstritten – schließlich handelt es sich dabei meist um die Standardeinstellung.

In der Praxis implementieren viele Anbieter momentan das für sie günstigere Opt-out-Prinzip, d.h. sie setzen weiterhin Tracking-Cookies ein, blenden auf ihren Seiten jedoch ein Informationsbanner ein, das die Nutzer über die Nutzung von Cookies informiert und ihnen eine Möglichkeit zum Widerspruch einräumt („Durch die Nutzung dieser Webseite erklären Sie sich mit der Verwendung von Cookies einverstanden. Um ihre Einwilligung zu widerrufen klicken Sie hier."). Problematisch ist dabei einerseits, dass die Nutzer ihren Widerruf auf jeder Webseite separat erklären müssen, und andererseits, dass der Widerspruch selbst wiederum in einem Cookie hinterlegt wird, also bei jedem Löschen der Cookies verloren geht. Mithin erleiden datenschutzsensible Nutzer einen zusätzlichen Komfortnachteil. Sinnvoller wäre es, auf den ausgereiften P3P-Standard zu setzen („Platform for Privacy Preferences", http://www.w3.org/P3P/), der sich trotz hoher Benutzerfreundlichkeit leider nicht durchgesetzt hat. P3P ermöglicht die Formulierung einer sowohl für Menschen verständlichen als von Maschinen automatisch auswertbaren Datenschutzerklärung auf Webseiten.

Zusammenfassend ist festzustellen, dass weder der DNT-Ansatz noch die EU-Cookie-Richtlinie bislang zu zufriedenstellenden Lösungen geführt haben.

6 Vorschläge für die Zukunft

Die Ausführungen haben deutlich gemacht, dass sich Internetnutzer beim Besuch von Webseiten kaum gegen unerwünschtes Tracking schützen können. Klassische Datenschutzkonzepte wie Einwilligung, Zweckbindung, Kontrolle und Transparenz sind derzeit nicht zufriedenstellend umgesetzt.

Glaubt man den Aussagen der Marketingindustrie, dann besteht kein Grund zur Sorge; schließlich seien die Webseitenbetreiber überhaupt nicht daran interessiert, mit den beim Tracking gesammelten Informationen die Identität einzelner Nutzer aufzudecken. Eine missbräuchliche Identifizierung sei höchstens theoretisch möglich, werde aber keinesfalls durchgeführt. Angesichts der hinterlistigen Methoden, derer sich die Werbenetze

in der Vergangenheit bedient haben, fällt es allerdings schwer, solchen Lippenbekenntnissen zu glauben.

Folglich sind die Nutzer auf technische und regulatorische Maßnahmen angewiesen, um ihre Datenschutzpräferenzen wirksam durchzusetzen. Dies gelingt nur, wenn Entwickler und Regulierer an einem Strang ziehen. Aus technischer Sicht sollte zunächst die Basis dafür geschaffen werden, dass die Tracking-Dienste zur Markierung bzw. zur Wiedererkennung nicht mehr Techniken zweckentfremden müssen, die ursprünglich für andere, wünschenswerte Zwecke konzipiert worden sind. In Anlehnung an die Android- und iOS-Plattformen könnten die Browser dazu mit einer dedizierten Tracking-ID ausgestattet werden, die vom Nutzer kontrolliert werden kann. Tracking durch missbräuchliche Verwendung anderer Techniken, z.B. durch HTTP-Cookies oder aktives Fingerprinting, könnte dann per Gesetz verboten und von den Aufsichtsbehörden verfolgt werden. Das rein passive Tracking (s. Abschnitt 4.3) lässt sich allerdings kaum gesetzlich verfolgen, da sein Einsatz überhaupt nicht nachweisbar ist. Hier sind also wiederum technische Lösungen gefragt.

Angesichts der zunehmenden Digitalisierung des Alltags wird der Schutz vor unerwünschter Beobachtung immer wichtiger. Die Sorge, dass wir aufgrund von automatisch erzeugten Verhaltensprofilen möglicherweise Nachteile erfahren könnten, ist durchaus berechtigt. Dabei sollten wir aber nicht die vielen erwünschten Identitäten aus den Augen verlieren, die wir im Laufe der Zeit durch die bewusste Preisgabe persönlicher Daten erschaffen haben.

Literatur

Abdelberi Chaabane, Kâafar Mohamed Ali and *Boreli Roksana* (2012): "Big friend is watching you: analyzing online social networks tracking capabilities", in: *Proceedings of the Workshop on Online Social Networks (WOSN'12)*, ACM, 7-12.

Acar Günes, Juarez Marc, Nikiforakis Nick, Diaz Claudia, Gürses Seda, Piessens Frank and *Preneel Bart* (2013): "FPDetective: Dusting the web for Fingerprinters", in: *Proceedings of the Conference on Computer and Communications Security (CCS'13)*, ACM, 1129-1140.

Acar Günes, Eubank Christian, Englehardt Steven, Juarez Marc, Narayanan Arvind and *Diaz Claudia* (2014): "The Web never forgets: Persistent tracking mechanisms in the wild", in: *Proceedings of the Conference on Computer and Communications Security (CCS'14)*, ACM, 674-689.

Ackermann, Elise (2013): *Google And Facebook Ignore 'Do Not Track Requests', Claim They Confuse Consumers*, http://www.forbes.com/sites/eliseackerman/2013/02/27/big-internet-companies-struggle-over-proper-response-to-consumers-do-not-track-requests/ (Abruf am 9.10.2014).

Angwin, Julia (2010): *The Web's New Gold Mine: Your Secrets*, http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html (Abruf am 9.10.2014).

Apple (2014): *ASIdentifierManager*, https://developer.apple.com/library/ios/documentation/AdSupport/Reference/ASIdentifierManager_Ref/ (Abruf am 9.10.2014).

Ayenson Mika, Wambach Dietrich James, Soltani Ashkan, Good Nathan and *Hoofnagle Chris Jay* (2011): *Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning,* http://ssrn.com/abstract=1898390 (Abruf am 9.10.2014).

Bager, Jo (2012): *Google umging auch die Cookie-Einstellungen des Internet Explorer*, http://heise.de/-1438459 (Abruf am 9.10.2014).

Beales, Howard (2009): *The Value of Behavioral Targeting*, http://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf (Abruf am 9.10.2014).

Becker, Tobias (2014): *Mobile Device Fingerprinting am Beispiel von Apples iOS*, Masterarbeit Univ. Erlangen-Nürnberg.

Berendt Bettina, Günther Oliver and *Spiekermann Sarah* (2005): "Privacy in e-commerce: stated preferences vs. actual behavior", in: *Communication of the ACM (CACM),* 48(4), 101-106.

BITKOM (2010): *Internetnutzer verwenden im Schnitt drei Mail-Adressen,* http://www.bitkom.org/de/markt_statistik/64026_62505.aspx (Abruf am 9.10.2014).

Clarke, Gavin (2013): *How the W3C met its Waterloo at the Do Not Track vote showdown*, http://www.theregister.co.uk/2013/11/05/do_not_track_w3c_ads_privacy/ (Abruf am 9.10.2014).

Dwoskin, Elizabeth (2014): Yahoo Won't Honor 'Do Not Track' Requests From Users, http://blogs.wsj.com/digits/2014/05/02/yahoo-wont-honor-do-not-track-requests-from-users/ (Abruf am 9.10.2014).

Eckersley, Peter (2010): "How Unique Is Your Web Browser?", in: Atallah, Mikhail J. and Hopper, Nicholas J. (Eds.), *Proceedings of the International Symposium on Privacy Enhancing Technologies (PETS'10)*, LNCS 6205, Heidelberg: Springer, 1-18.

Geary, Joanna (2012): *Tracking the trackers: What are cookies? An introduction to web tracking*, http://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro (Abruf am 9.10.2014).

Google (2014): *Advertising ID*, https://developer.android.com/google/play-services/id.html (Abruf am 9.10.2014).

Herrmann Dominik, Gerber Christoph, Banse Christian and Federrath Hannes (2010): "Analyzing Characteristic Host Access Patterns for Re-identification of Web User Sessions", in: Aura Tuomas, Järvinen Kimmo and Nyberg Kaisa (Eds.), *Proceedings of the Nordic Conference on Secure IT Systems (NordSec '10)*, LNCS 7127, Heidelberg: Springer, 136-154.

*Herrmann Dominik, Arndt Christine and Federrath Hanne*s (2012): "IPv 6 Prefix Alteration: An Opportunity to Improve Online Privacy", in: *Proceedings of the Workshop on Privacy and Data Protection Technology (PDPT'12)*.

Herrmann Dominik, Banse Christian and Federrath Hannes (2013): "Behavior-based Tracking: Exploiting Characteristic Patterns in DNS Traffic", in: *Computers & Security*, 39A, 17-33.

Hoffman Donna L., Novak Thomas P. and *Peralta Marcos* (1999): "Building consumer trust online", in: *Communications of the ACM (CACM)* 42(4), 80-85.

Hoofnagle, Chris Jay and *Good, Nathan* (2012): *The Web Privacy Census*, http://law.berkeley.edu/privacycensus.html (Abruf am 9.10.2014).

Hoofnagle Chris Jay, Soltani Ashkan, Good Nathan, Wambach Dietrich J. and *Ayenson Mika* (2012): "Behavioral Advertising: The Offer You Cannot Refuse", in: *Harvard Law & Policy Review* 6, 273-296.

Juels Ari, Jakobsson Markus and *Jagatic Tom N. (2006*): "Cache Cookies for Browser Authentication (Extended Abstract)", in: *Proceedings of the Symposium on Security and Privacy (S&P'06)*, IEEE Computer Society, 301-305.

Kleindl, Michael und *Theobald, Axel* (1999): „Werbung im Internet", in: Bliemel Friedhelm, Fassott Georg and Theobald Axel (Hrsg.), *Electronic Commerce*, Wiesbaden: Gabler Verlag, 281-296.

Kohno Tadayoshi, Broido Andre and *Claffy Kimberly C*. (2005): "Remote Physical Device Fingerprinting", in: *Proceedings of the Symposium on Security and Privacy (S&P),* IEEE Computer Society, 211-225.

Kramera Adam D. I., Guillory Jamie E. and *Hancock Jeffrey T.* (2013): "Experimental evidence of massive-scale emotional contagion through social networks", in: *Proceedings of the National Academy of Sciences (PNAS)* 111(24), 8788-8790.

Kurtz, Andreas (2014): *Malicious iOS Apps,* http://www.andreas-kurtz.de/2014/09/malicious-apps-ios8.html (Abruf am 9.10.2014).

Lavin, Marilyn (2006): "Cookies: What do consumers know and what can they learn. Journal of Targeting", in: *Measurement and Analysis for Marketing* 14(4), 279-288.

Lindqvist Janne and *Tapio Juha-Matti* (2008): "Protecting Privacy with Protocol Stack Virtualization", in: *Proceedings of the Workshop on Privacy in the Electronic Society (WPES'08)*, ACM, 65-74.

Lischka, Konrad (2011): *Streit über Internet-Pseudonyme: Die Ignoranz der Mehrheit,* http://www.spiegel.de/netzwelt/netzpolitik/streit-ueber-internet-pseudonyme-die-ignoranz-der-mehrheit-a-778988.html (Abruf am 9.10.2014).

Mattioli, Dana (2012): *On Orbitz, Mac Users Steered to Pricier Hotels*, http://online.wsj.com/news/articles/SB10001424052702304458604577488822667325882 (Abruf am 9.10.2014).

Mayer, Jonathan R. (2013): "The New Firefox Cookie Policy", in: *ACM Crossroads*, 20(1), 16-17.

Mayer, Jonathan R. and *Mitchell, John C*. (2012): "Third-party web tracking: Policy and technology", in: *Proceedings of the Symposium on Security and Privacy (S&P'13)*, IEEE Computer Society, 413-427.

McDonald, Aleecia M and *Cranor, Lorrie F*. (2010): "Americans' attitudes about internet behavioral advertising practices", in: *Proceedings of the Workshop on Privacy in the Electronic Society (WPES'10)*, ACM, 63-72.

Mowery, Keaton and *Shacham, Hovav* (2012): "Pixel Perfect: Fingerprinting Canvas in HTML5", in: *Proceedings of the Web 2.0 Security and Privacy 2012 Workshop (W2SP)*, *San Francisco,* IEEE Computer Society.

Mowery Keaton, Bogenreif Dillon, Yilek Scott and *Shacham Hovav* (2011): "Fingerprinting information in JavaScript implementations", in: *Proceedings of the Web 2.0 Security and Privacy 2011 Workshop (W2SP), San Francisco*, IEEE Computer Society.

Nikiforakis Nick, Kapravelos Alexandros, Joosen Wouter, Kruegel Christopher, Piessens Frank and *Vigna Giovanni* (2013): "Cookieless Monster: Exploring the Ecosystem of Web-Based Device Fingerprinting", in: *Proceedings of the Symposium on Security and Privacy (S&P'13)*, IEEE Computer Society, 541-555.

*Nissenbaum, Helen (*2004): "Privacy as Contextual Integrity", in: *Washington Law Review*, 79(1), 119-158.

Oestreich, Nicolas (2014): *So eindeutig lässt sich jedes iPhone zuordnen,* http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244/ (Abruf am 9.10.2014).

Pariser, Eli (2011): *The Filter Bubble: What the Internet Is Hiding from You*, London: Viking/Penguin Press.

Roesner Franziska, Kohno Tadayoshi and *Wetherall David* (2012): "Detecting and Defending Against Third-Party Tracking on the Web", in: *Proceedings of the Conference on Networked Systems Design and Implementation (NSDI'12), San José, CA,* USENIX Association, 155-168.

Schmundt, Hilmar (2012): *Die Keks-Spione,* http://www.spiegel.de/spiegel/print/d-84519398.html (Abruf am 9.10.2014).

Singer, Natasha (2012): *You for Sale: Your Online Attention, Bought in an Instant,* http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html (Abruf am 9.10.2014).

Soltani Ashkan, Canty Shannon, Mayo Quentin, Thomas Lauren and *Hoofnagle Chris J.* (2009): *Flash Cookies and Privacy* http://ssrn.com/abstract=1446862 (Abruf am 9.10.2014).

Temple, James (2014): *Mozilla anticookie tool plans crumbling,* http://www.sfgate.com/technology/dotcommentary/article/Mozilla-anticookie-tool-plans-crumbling-4958045.php (Abruf am 9.10.2014).

Turow, Joseph (2011): *The daily you: how the new advertising industry is defining your identity and your world*, New Haven: Yale University Press.

Ur Blase, Leon Pedro G., Cranor, Lorrie F., Shay Richard and *Wang Yang* (2012): "Smart, useful, scary, creepy: perceptions of online behavioral advertising", in: *Proceedings of the Symposium On Usable Privacy and Security (SOUPS'12),* ACM.

Yan Jun, Shen Dou, Mah Teresa, Liu Ning, Chen Zheng and *Li Ying* (2011): "Behavioral Targeting Online Advertising", in: Hua Xian-Sheng, Mei Tao and Hanjalic Alan (Eds.), *Online Multimedia Advertising: Techniques and Technologies*, IGI Global, 213-232.

Rechtliche Perspektiven des Identitätsmanagements in Europa

Gerrit Hornung

1 Identitäten im Nationalstaat und in Europa

Mit dem Begriff der „Identität" lassen sich einerseits sehr konkrete Dinge, andererseits sehr offene Konzepte bezeichnen.[1] Der Terminus „Identitätsmanagement" fällt in aller Regel in die erste Kategorie und umschreibt technische und soziale Vorgänge des vertrauenswürdigen Informationsaustauschs. Die entsprechenden technischen Konzepte dienen dem Nachweis, dass man eine bestimmte Person (als Entität)[2] ist beziehungsweise eine bestimmte Eigenschaft oder Berechtigung hat. Diese Informationen werden als digitale Repräsentation einer Person in Form von Daten verarbeitet.[3] Auch aus einer rechtlichen Perspektive bezeichnet Identitätsmanagement in aller Regel ein Identifizierungs-, Attributs- und/oder Berechtigungsmanagement.[4] Letztlich handelt es sich damit um ein Element und eine Basisstruktur der zwischenmenschlichen Kommunikation. In Form der unmittelbaren Interaktion und individuellen menschlichen kognitiven Leistung ist diese Basisstruktur schon sehr alt. Im hier verstanden Sinne wird sie jedoch vielfach technisch unterstützt oder sogar mehr oder weniger vollständig automatisiert.

Wie andere Formen individueller und gesellschaftlicher Kommunikation kann auch das Identitätsmanagement in rechtlicher Hinsicht regulie-

---

1 S. zusammenfassend Hornung 2005: 29 ff. m.w.N.

2 Mit diesem neutralen Begriff kann man bezeichnen, dass Identitätsmanagement sich auch auf Organisationen, Tiere, Sachen oder beliebige sonstige Objekte beziehen kann. Diese Perspektive wird im Folgenden ausgeklammert.

3 Zur Terminologie s. die instruktive Übersicht bei Pfitzmann und Hansen 2010, v.a. 29 ff.; s. ferner Baier 2006; ULD Schleswig-Holstein und TU Dresden 2007: 22 ff.; Hühnlein 2008: 163. Mit dem Zusammenspiel zwischen Identitätsmanagement und Datenschutz befasst sich inzwischen auch die Standardisierungsgruppe ISO/IEC JTC 1/SC 27/WG 5 „Identity management and privacy technologies" (s. dazu den Beitrag von Schallaböck in diesem Band).

4 Zu verschiedenen Formen des Identitätsmanagements aus rechtlicher Sicht s. Hornung 2015b: 189 ff.

rungsbedürftig sein. Daraus resultieren die Fragen, wer für diese Regulierung zuständig ist, welche Elemente des Identitätsmanagements geregelt werden sollten, und in welcher Weise diese auszugestalten sind.

Die Zuständigkeitsfrage ist dabei von besonderer Bedeutung, weil Identität als „behördliche Identität“[5] auf das engste mit dem Verhältnis zwischen Staat und Bürger, dem Zugriff des Staates auf die Körper der Staatsangehörigen, dem Zugang zu staatlichen Leistungen und der Teilhabe an staatlichen Entscheidungsprozessen verknüpft ist.[6] Letztlich geht es also (auch) um Grundfragen der staatlichen Gemeinschaft und der Zugehörigkeit zu ihr.

Die Entscheidung über diese Fragen – und damit über Identität, Identifizierung und Identitätsmanagement – sind historisch gesehen nationalstaatliche Aufgaben.[7] Diese Zuordnung wird jedoch in Zeiten der Entstehung und Verfestigung supranationaler Verbindungen wie der Europäischen Union und der weltweiten technischen und ökonomischen Vernetzung durch das Internet zunehmend prekär. Der folgende Beitrag geht deshalb aus einer rechtlichen Perspektive den globalen Trends des Identitätsmanagements nach und analysiert im Detail die Kompetenzverteilungen in der Europäischen Union.

2 Europäische und weltweite Strukturen

In der Europäischen Union ist ein klarer Trend erkennbar, die technischen, rechtlichen und sozialen Fragen des Identitätsmanagements zu europäisieren. Die Gründe für diesen Trend sind einerseits politisch-rechtlicher, andererseits technischer Natur.

2.1 Gründe der zunehmenden Europäisierung

Politisch und rechtlich tritt die Europäische Union seit vielen Jahren als eigentümliches, oftmals als „supranational“ bezeichnetes Gebilde zwar nicht

5 Zu dieser Perspektive Bogdanowicz und Beslay 2001.

6 S. z.B. Engemann 2012: 205 ff.; s.a. Hornung 2011: Rn. 1 ff.; für das Beispiel Indiens s. von Damm (in diesem Band).

7 S. zu den Ursprüngen Groebner 2004; zur historischen Entwicklung s. den Beitrag von Engemann in diesem Band.

vollständig, wohl aber teilweise an die Stelle der Nationalstaaten. Diese haben in weiten Bereichen die Kompetenz zur Normsetzung an die Union delegiert und es überdies praktisch immer toleriert, wenn die Unionsorgane diese Kompetenzen sehr weit interpretieren. Der Grad der Vergemeinschaftung variiert nach dem jeweiligen Rechtsgebiet. Während die wirtschaftlichen Aktivitäten im europäischen Binnenmarkt inzwischen sehr stark durch die Unionsgesetzgebung reguliert werden, bewahren die Mitgliedstaaten in „klassischen" staatlichen Bereichen vielfach ihre herkömmlichen Kompetenzen. Beispiele bilden Fragen der Außen- und Sicherheitspolitik, des Straf- und Strafverfahrensrechts, der Sozialpolitik sowie der Steuererhebung und Budgetverantwortlichkeit.

Das Identitätsmanagement befindet sich hier in einer mittleren Position. Die Grundfrage der Zugehörigkeit zur Gemeinschaft in Form der Staatsbürgerschaft wird nach wie vor ausschließlich durch die Mitgliedstaaten entschieden. Auch für die nationalen Bevölkerungsregister gibt es keine unionsweiten Vorgaben.[8] In vielen anderen Bereichen existieren demgegenüber europäische Regelungen. Die Beispiele reichen von sehr offenen und normativ noch wenig ausgeformten, symbolisch hingegen aufgeladenen Konstrukten wie der Unionsbürgerschaft der Europäischen Union[9] bis hin zu sehr spezifischen technischen Standards bei europaweit einheitlichen biometrischen Reisepässen[10] oder technischen Vorgaben zur Interoperabilität nationaler Identifizierungsinfrastrukturen für das Internet.[11] Auch die Kooperation im Schengen-Raum ist ein Beispiel für die Übertra-

---

8 In einigen Staaten wie dem Vereinigten Königreich existiert nach wie vor überhaupt kein Melderegister. Die Europäische Kommission hat ein Projekt zur europaweiten elektronischen Melderegisterauskunft gefördert, das nunmehr kommerziell angeboten wird (www.riserid.eu/). Dieses betrifft aber nur den Austausch existierender Daten, deren Umfang und Inhalt die Mitgliedstaaten bestimmen.

9 Die Unionsbürgerschaft ist keine eigene Staatsangehörigkeit, sondern folgt der Angehörigkeit zu einem Mitgliedstaat, s. Art. 9 Satz 2, 3 EUV und Art. 20 Abs. 1 AEUV. In ihr werden Rechte der Unionsbürgerinnen und Unionsbürger gebündelt, die in anderen Bereichen des Europarechts gewährt werden; s. näher z.B. die Beiträge in Schroeder und Obwexer 2015.

10 Verordnung (EG) Nr. 2252/2004 v. 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. EU Nr. L 385 v. 29.12.2004; geändert durch die VO (EG) Nr. 444/2009, ABl. EU Nr. L 142 v. 6.6.2009, s. Roßnagel und Hornung 2005: 983 ff.; monographisch Pallasky 2007: 30 ff.; Altmann 2010, passim; zu den völker- und europarechtlichen Bezügen s. Hornung 2011: Rn. 10 ff.

11 S.u. 3.1 bis 3.3 sowie den Beitrag von Bender in diesem Band.

gung einer staatlichen Kernkompetenz – wenn auch bisher überwiegend nicht an die Union, sondern untereinander an andere Mitgliedstaaten.[12] Der Wegfall der Identitätskontrolle an Binnengrenzen bedeutet für mehrere Mitgliedstaaten (insbesondere auch für Deutschland), dass nur noch an Flug- und Seehäfen das an sich ureigene staatliche Recht wahrgenommen wird, den Zugang zum Staatsgebiet zu kontrollieren.[13]

Der zweite Grund für die zunehmende Zentralisierung in Europa ist technischer Natur. Praktisch alle entscheidungsbedürftigen technischen und organisatorischen Fragen des elektronischen Identitätsmanagements sind nicht auf einzelne staatliche Territorien beschränkt. Dies gilt unabhängig davon, ob derartige Systeme durch staatliche oder private Betreiber angeboten werden. In einem wirtschaftlichen Binnenmarkt ist es weder sinnvoll noch den Bürgern zu vermitteln, wenn Authentisierungsinstrumente ausschließlich bei Anbietern in einem einzigen Mitgliedstaat einsetzbar sind. Dies gilt schon für den Zugang zu Behörden, wenn beispielsweise Bürger oder Unternehmen in anderen Mitgliedstaaten eine Dienstleistung anbieten und dafür eine behördliche Genehmigung benötigen. Im Bereich des E-Commerce ist das Problem noch größer, weil die Kunden hier viel häufiger grenzüberschreitend Waren und Dienstleistungen in Anspruch nehmen. Aus der Perspektive der Anbieter der Internetwirtschaft ist ein Flickenteppich aus nicht interoperablen Systemen sogar prohibitiv, weil der Implementierungsaufwand für jedes einzelne System sich betriebswirtschaftlich nicht rechtfertigen lässt.

Bei weltweit operierenden privaten Anbietern kommt hinzu, dass selbst wirtschaftsstarke EU-Mitgliedstaaten wie Deutschland nicht wichtig genug sind, um mit rein faktischen Standards den Markt signifikant zu beeinflussen. So könnte beispielsweise der elektronische Identitätsnachweis

12 Der europäische Beitrag zur Kontrolle an den Schengen-Außengrenzen wird stetig größer. Dies betrifft insbesondere die Europäische Grenzagentur Frontex (dazu umfassend Lehnert 2014), die ursprünglich ausschließlich im Bereich von Organisation, Koordination und technischer Unterstützung tätig war, inzwischen aber – in Zusammenarbeit mit den Ländern vor allem Südosteuropas – mehr und mehr operative Tätigkeitsfelder besetzt.

13 Dies gilt – wie sich seit dem Sommer 2015 in aller Deutlichkeit gezeigt hat – vorbehaltlich der Stichprobenkontrolle (Art. 21 des Schengener Grenzkodex), der ausnahmsweisen vorübergehenden Wiedereinführung von Grenzkontrollen (Art. 23 ff.) und Hilfsinstrumenten wie der so genannte Schleierfahndung (z.B. nach Art. 13 Abs. 1 Nr. 5, Abs. 2 BayPAG).

des neuen Personalausweises[14] selbstverständlich durch global agierende Anbieter wie Amazon und eBay eingesetzt werden. Dies würde die Identifizierungs- und Transaktionssicherheit signifikant erhöhen und damit die durch unsichere Verfahren erzeugten finanziellen Schäden reduzieren, die derzeit häufig auf dem Kulanzwege reguliert und damit über entsprechende Preise und Gebühren auf alle Kunden umgelegt werden. Der Implementierungsaufwand allein für den deutschen Markt ist aber ganz offensichtlich so hoch, dass die Anbieter diesen Weg nicht gehen.

Ob rechtlich verbindliche einheitliche Standards beispielsweise für nationale elektronische Ausweise[15] dieses Problem lösen werden, bleibt abzuwarten, weil die Marktdurchdringung noch von vielen weiteren Faktoren abhängt.[16] Die Chancen hierfür sind aber jedenfalls deutlich größer als bei nationalen Insellösungen.

2.2 Möglichkeiten und Grenzen weltweiter Strukturen

Das Bedürfnis nach interoperablen, allgemein anwendbaren Systemen des Identitätsmanagements lässt sich grundsätzlich nicht nur innerhalb Europas, sondern weltweit feststellen. Die Internetwirtschaft ist vielfach nicht nur kontinental, sondern global verflochten. Überdies werden viele Märkte von weltweit agierenden Anbietern dominiert, die ihren Sitz nur selten innerhalb der Europäischen Union haben, sondern typischerweise in den USA. Derartige international tätige Unternehmen würden von einer weltweiten Standardisierung erheblich profitieren. Überdies sind es auch die Nutzer zunehmend gewohnt, zumindest bei Dienstleistungen weniger auf den Unternehmenssitz zu schauen. Das gilt beispielsweise für Angebote des Cloud Computings.

2.2.1 Interkontinentale Gegensätze

Ungeachtet dieser Ausgangssituation sind die Unterschiede zwischen den staatlichen Regulierungsansätzen im weltweiten Vergleich (beispielsweise

---

14 Zu diesem s. Roßnagel et al. 2008: 168; Roßnagel und Hornung 2009: 301; Schulz 2009: 267; Polenz 2010: 671; Borges 2010: 3334; Möller 2011: Rn. 3 ff.

15 S. dazu unten 3.1 bis 3.3.

16 S. z.B. den Beitrag von Roßnagel et al. in diesem Band.

zwischen den USA und Deutschland)[17] noch größer als innerhalb Europas.[18] Wirklich verwunderlich ist dies nicht: Trotz des Zusammenwachsens der weltweiten Internetwirtschaft ist diese weit von einem globalen Binnenmarkt entfernt. Wie groß die Unterschiede selbst zwischen soziokulturell relativ ähnlichen Staaten sein können, lässt sich derzeit am Beispiel der Verhandlungen über das Transatlantische Freihandelsabkommen TTIP beobachten. Dementsprechend existiert kein rechtlicher Rahmen für ein weltweites elektronisches Identitätsmanagement und auch keine Organisation, die für die Ausarbeitung derartiger Regeln zuständig ist.[19]

Während auf technischer Ebene durchaus weltweit gültige Standards beispielsweise für Public Key Infrastrukturen (PKI) existieren, die sich für elektronische Signaturen und die elektronische Authentisierung nutzen ließen, fehlt es also an einer Instanz, die beispielsweise verbindlich vorgeben könnte, wer als Anbieter auftritt (Staat oder – mehr oder weniger regulierte – Private), wie hoch die Anforderungen an die Erstidentifizierung sein sollen, ob für unterschiedliche Anwendungsszenarien differenzierte Sicherheitsniveaus angewendet werden können, welche datenschutzrechtlichen Anforderungen zu beachten sind oder wie etwaige Haftungsfragen gelöst werden.

Weltweit fehlt es allerdings nicht nur rechtlich, sondern zumindest bislang auch faktisch an Akteuren, die entsprechende Standards durchsetzen können. Nach den Anschlägen des 11. September 2001 entfalteten die USA erheblichen politischen Druck auf andere Staaten, um diese zur Einführung biometrischer Reisedokumente zu bewegen.[20] Vergleichbare Aktivitäten hat es im Bereich des elektronischen Identitätsmanagements nicht gegeben, obwohl die USA durchaus über eine durch Präsident Obama abgesegnete nationale Strategie zur Förderung und Verbreitung entsprechen-

17 S. dazu Rosner 2014; Engemann 2015: 43 ff.; s. ferner Knight und Saxby 2014: 617 ff.

18 S. zu Europa insoweit Kubicek und Noack 2010.

19 Eine Ausnahme bildet die International Civil Aviation Organization (ICAO), die als zivile Luftfahrbehörde der Vereinten Nationen weltweit die technischen Spezifikationen für Reisedokumente verabschiedet (s. aus rechtlicher Sicht näher Schäffer 2007). Hierbei handelt es sich aber um einen begrenzten Anwendungsfall, der insbesondere keine Auswirkungen auf den Internet-Bereich hat.

20 Gegenüber 25 mit den USA engen Verbündeten Staaten bestand das Druckmittel in der (gesetzlich im Enhanced Border Security and Visa Reform Act fixierten) Drohung, das Visa-Waiver-Abkommen aufzukündigen, das es Staatsangehörigen ermöglicht, ohne Visum in die USA einzureisen.

der Systeme verfügen (NSTIC).[21] In diesem Rahmen sind seit dem Jahre 2011 Stakeholder aus Wirtschaft, Verwaltung und Zivilgesellschaft eingeladen, Standards und Verfahren des Identitätsmanagements zu entwickeln. Mit belastbaren Ergebnissen ist im Jahre 2017 zu rechnen.[22]

Ein direkter Druck auf andere Staaten dürfte insoweit allerdings auch in Zukunft wenig wahrscheinlich sein, weil Fragen der Registrierung und Wiedererkennung der Bürger eine ureigene nationalstaatliche Aufgabe darstellen, die entsprechenden Vertrauensanker (Personenstandsregister) sehr heterogen ausgestaltet sind und keine Einigkeit über die Notwendigkeit einer „starken", staatlich gesteuerten Authentisierung im Internet besteht. Eine indirekte Regulierung wäre den USA dagegen mutmaßlich möglich, wenn hierzu ein politischer Wille bestünde: Würden sie den dort ansässigen großen Internetanbietern verbindliche Vorgaben zur Identifizierung ihrer Kunden und zum Umgang mit den Identitätsdaten machen, wäre es nicht unwahrscheinlich, dass die Anbieter diese konzern- und damit weltweit implementieren würden.

2.2.2 Privatwirtschaftliche Akteure

In Abwesenheit verbindlicher Vorgaben haben private Akteure wie Facebook Modelle entwickelt, um als Identitätsprovider aufzutreten.[23] Sie verwenden dabei die Identitätsdaten ihrer Nutzer, die im Rahmen des Registrierungsprozesses oder im Anschluss erhoben werden, und stellen diese auf unterschiedliche Art und Weise anderen Anbietern zur Verfügung, damit letztere auf eigene Registrierungs- und Authentisierungsverfahren verzichten können. Es handelt sich typischerweise um private Unternehmen mit weltweitem Operationsgebiet. Aufgrund der hohen Nutzerzahlen (insbesondere bei Facebook) erreichen sie schnell eine kritische Masse, die sie für den Markt interessant werden lässt.

Intuitiv wird man derartigen Identitätsmanagementsystemen ein geringeres Maß an Identifizierungssicherheit beimessen. Bei näherer Analyse ist dies freilich differenziert zu bewerten. Zwar fehlt es an gesetzlich begründeten und standardisierten Identifizierungspflichten. Private Anbieter

---

21 S. The White House 2011; näher Engemann 2015: 43, 57 ff.

22 Zu Zwischenergebnissen s. http://www.nist.gov/nstic.

23 Zum Verhältnis von staatlichen und privaten Strukturen des elektronischen Identitätsmanagements s. aus rechtlicher Sicht Hornung 2015b: 204 ff.

haben aber durchaus die Möglichkeit, über Verfahren wie PostIdent, das postalische Zusenden von Zugangsdaten oder andere Mechanismen ihre Kunden relativ gut zu identifizieren. Derartige Prozesse lassen sich durch Vertragsklauseln ebenso absichern wie die (in Deutschland) rechtlich umstrittene Klarnamenpflicht bei den Profilen in sozialen Netzwerken.[24]

Insbesondere die Anbieter von Social Media verfügen über ein weiteres Instrument, um die Echtheit der entsprechenden Daten zu bewerten: Sie können hierzu Kommunikationsinhalte analysieren. Eine Erstregistrierung mit falschen Angaben über Namen, Geburtstag oder andere Informationen dürfte bei „normaler" Benutzung der Netzwerke nur mit hohem Aufwand dauerhaft gegenüber den Anbietern durchzuhalten sein – wer kann schon verhindern, dass persönliche Kontakte am tatsächlichen Geburtstag unter Verwendung des Klarnamens gratulieren? Da die Anbieter die kommunikative Nutzung protokollieren (können), können sie auch abschätzen, wie gut das Identifizierungsniveau im konkreten Einzelfall ist. Aus dieser Information lässt sich sogar ein Geschäftsmodell entwickeln, wenn die Empfänger der Identitätsdaten ein bestimmtes Sicherheitsniveau anfordern.

In Europa dürfte es unrealistisch und in den meisten Mitgliedstaaten rechtlich unzulässig sein, auf dieser Basis staatliche Verwaltungsverfahren abzuwickeln. In anderen Regionen mag sich dies jedoch anders darstellen, und in der Privatwirtschaft gibt es ganz offensichtlich genügend Betreiber von Webseiten, für die das angebotene Sicherheitsniveau akzeptabel ist.

Ob sich derartige weltweite, rein marktförmige Lösungen durchsetzen können, bleibt dennoch abzuwarten. Gegenüber Negativbeispielen wie Microsofts CardSpace[25] schienen zwischenzeitlich offene, dezentrale Systeme wie OpenID erfolgreicher zu sein. Derzeit laufen ihnen allerdings anscheinend kommerzielle Angebote wie Facebook Login den Rang ab,[26] auch wenn ihr endgültiger Erfolg wie bei anderen Lösungen von verschiedenen Angebots- und Nachfragefaktoren abhängig ist.[27]

---

24 Dazu Schnabel und Freund 2010: 718 ff.; Stadler 2011: 57 ff.; s.a. Hornung 2015a: Rn. 93 ff.

25 Die Entwicklungsarbeit wurde am 15.2.2011 eingestellt, s. http://blogs.msdn.com/b/card/archive/2011/02/15/beyond-windows-cardspace.aspx; zum Nachfolgeprojekt „U-Prove" s. http://research. microsoft.com/en-us/projects/u-prove/.

26 S. z.B. Mims 2010.

27 S. den Beitrag von Roßnagel et al. in diesem Band.

Jenseits der Frage, ob Facebook Login datenschutzrechtlich zulässig ist oder gestaltet werden kann,[28] stellt sich jedenfalls das grundlegende Problem, dass Anbieter von sozialen Netzwerken wie Facebook ihr gesamtes Geschäftsmodell darauf ausrichten, personenbezogene Daten ihrer Kunden zu sammeln.[29] Sollten sich derartige Anbieter als Identitätsprovider durchsetzen, so wäre dies ein – weiterer – Grund daran zu zweifeln, dass der Markt selbst in der Lage ist, datenschutzfreundliche Identitätsmanagement-Lösungen hervorzubringen.

3 Kompetenzverteilungen und faktischer Einfluss innerhalb der Europäischen Union

Innerhalb der Europäischen Union lassen sich derzeit erhebliche Veränderungen der Regulierung von Fragen des Identitätsmanagements beobachten. Diese erfassen sowohl Kompetenzen als auch inhaltliche Standards. Während Angebote wie Facebook Login auch in Europa rechtlich nicht spezifisch reguliert sind, finden sich inzwischen mehrere Systeme, für die die jeweiligen Gesetzgeber ein definiertes Maß an Sicherheit und Datenschutz anstreben. Die Europäische Union hat hier in den letzten Jahren deutlich Aktivitäten zur Vereinheitlichung entfaltet, die jedoch neue Rechtsfragen aufwerfen.

3.1 Erzeugung von Identitäten

Während die originäre Erzeugung von Identitäten im Sinne der Zugehörigkeit zur staatlichen Gemeinschaft (Staatsangehörigkeitsrecht) immer noch praktisch ausschließlich in der Zuständigkeit der Mitgliedstaaten liegt,[30] macht die Europäische Union inzwischen in anderen Bereichen relativ präzise Vorgaben. Für den Pass bestehen verbindliche Regelungen, deren

---

28 Dazu Moser-Knierim 2013: 263 ff.

29 S. zu den datenschutzrechtlichen Fragen sozialer Netzwerke Hornung 2015a: 79 ff.

30 Das gilt sowohl für den ursprüngliche Erwerb qua Geburt, für den in Europa nach wie vor diverse Abwandlungen und Mischformen der Grundprinzipien des ius sanguinis (Abstammungsprinzip; so herkömmlich in Deutschland) und ius soli (Geburtsortsprinzip) existieren, als auch hinsichtlich der Voraussetzungen für eine Einbürgerung. Für beides macht das Unionsrecht keine Vorgaben; zu den – wenigen – Vorgaben des Völkerrechts s. insoweit Hailbronner 2010: Rn. 6 ff.

wichtigste die Pass-Verordnung (EG) Nr. 2252/2004 zur Ausgestaltung des neuen Passes mit elektronischem Speichermedium und biometrischen Daten ist.[31] Demgegenüber verfügt die Union erst seit dem Inkrafttreten des Vertrags von Lissabon über eine Regelungskompetenz zum Erlass von Bestimmungen für Personalausweise (Art. 77 Abs. 3 AEUV). Dementsprechend findet die Pass-Verordnung gemäß Art. 1 Abs. 3 Satz 2 auch keine Anwendung auf Personalausweise der Mitgliedstaaten.[32]

Die neue Kompetenz in Art. 77 Abs. 3 AEUV setzt explizit voraus, dass ein Tätigwerden der Union erforderlich ist, um die Ausübung des in Art. 20 Abs. 1 Satz 2 lit. a AEUV gewährleisteten Rechts der Unionsbürger zu erleichtern, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten. Die Norm erfasst also Fragen der Grenzkontrolle und der physischen, nicht der elektronischen Mobilität der Unionsbürger.[33] Folgerichtig stützt sich die neue Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG[34] (so genannte eIDAS-VO)[35] nicht auf Art. 77 Abs. 3 AEUV, sondern auf die allgemeine Binnenmarktkompetenz des Art. 114 AEUV.[36]

---

31 S.o. Fn. 10.

32 Dieses angesichts des Wortlauts und der fehlenden Kompetenz bei Verabschiedung an sich selbstverständliche Ergebnis hat der EuGH explizit festgestellt, s. EuGH, Rs. C-446/12 u.a. – Willems, ZD 2015, 420.

33 S.a. Andrade 2012: 158 f.

34 ABl. EU Nr. L 257/73 v. 28.8.2014; s. z.B. Roßnagel 2014: 3686 ff; 2015: 359 ff.; zum Kommissionsentwurf z.B. Dumortier und Vandezande 2012; Quiring-Kock 2013: 20 ff.; Roßnagel und Johannes 2013; 65 ff.; Spindler und Rockenbauch 2013; 139 ff.; Hornung 2015b: 213 ff; zu Problemen dieses Entwurfs in Bezug auf das Identitätsmanagement s. Hornung 2012a: 633 f.; Sädtler 2013; Quiring-Kock 2013: 21 ff.; Spindler und Rockenbauch 2013: 141 ff.; Hoffmann 2014: 764 f.; zu den beweisrechtlichen Fragen s. Jandt 2015: 1205 ff.

35 eIDAS steht für electronic Identification, Authentication and Signature. Da die Abkürzung auch für die Übersetzung funktioniert, hat sie sich in der deutschen Diskussion ebenfalls etabliert.

36 S. umfassend zu den entsprechenden Kompetenzen Andrade 2012, der für elektronische Identitäten eine Kompetenz auf der Basis einer Zusammenschau von Art. 3 EUV und Art. 26, 114 AEUV befürwortet. Die ebenfalls von Andrade (2012: 161) vorgeschlagene Fundierung im Datenschutzrecht ist hingegen eine erhebliche Überdehnung, weil dieses eine Querschnittsmaterie ist und eine solchen Herangehensweise Kompetenzen für eine Vielzahl weiterer Gesetzgebungsaktivität der Union begründen könnte.

Die geltende Signaturrichtlinie[37] stützt sich auf dieselbe Kompetenznorm. Sie regelt nur rudimentär die Anforderungen an die Erzeugung elektronischer Identitäten, die für die Authentizität der qualifizierten elektronischen Signatur bürgen. Im Rahmen der Umsetzung der Richtlinie hat Deutschland in § 5 SigG und § 3 SigV deutlich detailliertere Vorgaben für die Erstidentifizierung des Signaturschlüssel-Inhabers und den Nachweis von Attributen normiert.[38]

Nunmehr macht die Union spezifische Vorgaben für die Erstidentifizierung. Art. 24 Abs. 1 eIDAS-VO regelt die Voraussetzungen für die Vergabe qualifizierter Zertifikate. Qualifizierte Vertrauensdiensteanbieter[39] müssen sich mittels definierter Vorgehensweisen von der Identität und gegebenenfalls spezifischen Attributen der natürlichen oder juristischen Person überzeugen, für die sie ein qualifiziertes Zertifikat ausstellen. Dies kann erfolgen

- durch persönliche Anwesenheit des Antragstellers (dann regelmäßig unter Vorlage eines staatlichen Identitätspapiers),
- durch ein elektronisches Identifizierungsmittel des Sicherheitsniveaus „substantiell“ oder „hoch“,
- durch ein Zertifikat einer qualifizierten elektronischen Signatur oder eines qualifizierten elektronischen Siegels, oder
- durch eine national anerkannte Identifizierungsmethode mit gleichwertiger Sicherheit.

Hierdurch wird ein nachprüfbar hohes Niveau für die Sicherheit der Erstidentifizierung sichergestellt, die als Vertrauensanker für das gesamte System dient. Zwar enthält die Verordnung keine Pflicht der Mitgliedstaaten, lediglich Identifizierungssysteme einzuführen, die einem der drei Sicherheitsniveaus (neben „hoch“ und „substantiell“ noch „niedrig“) entsprechen. Es besteht also kein Verbot, Vertrauensdienste mit einem niedrigeren Sicherheitsniveau oder auch Zwischenstufen anzubieten. Diese liegen dann jedoch außerhalb des Anwendungsbereichs der Verordnung und ge-

---

37 Richtlinie 1999/93/EG v. 13.12. 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG Nr. L 13/12 v. 19.1.2000.

38 S. näher Hornung 2013b: Rn. 17 ff.

39 Dies sind neben den bisherigen Zertifizierungsdiensteanbietern nach Art. 2 Nr. 11 der Signaturrichtlinie und § 2 Nr. 8 SigG Anbieter von elektronischen Siegeln, Zeitstempeln, Einschreiben, Website-Authentifizierung und Aufbewahrungsangeboten.

nießen nicht die in ihr definierten Rechtsfolgen.[40] Insbesondere ist die Einhaltung eines der drei Niveaus nach Art. 7 lit. c eIDAS-VO Voraussetzung für die Notifizierung. Da nur notifizierte nationale elektronische Identifizierungssysteme von anderen Mitgliedstaaten anerkannt werden müssen,[41] besteht ein erheblicher faktischer Anreiz, die entsprechenden technischen Spezifikationen einzuhalten.

Mit den Sicherheitsniveaus „niedrig", „substantiell" und „hoch" regelt die eIDAS-Verordnung erstmals auf europäischer Ebene Einzelheiten für elektronische Identifizierungsmittel, die dem Zweck der Authentisierung dienen. Die drei Sicherheitsniveaus werden in Art. 8 eIDAS-VO und entsprechenden Durchführungsrechtsakten der europäischen Kommission spezifiziert.[42] Die technischen Spezifikationen, Normen und Verfahren befassen sich vor allem mit der Erzeugung elektronischer Identitäten. Geregelt werden insbesondere Verfahren zum Nachweis und zur Überprüfung der Identität natürlicher und juristischer Personen, das Verfahren der Ausstellung, Details zur Einrichtung, die die Identifizierungsmittel ausstellt sowie technische und sicherheitsbezogene Spezifikationen der ausgestellten elektronischen Identifizierungsmittel.[43]

Als weitere Anforderung an die Erstidentifizierung und Voraussetzung der Notifizierung verpflichtet Art. 7 lit. d eIDAS-VO den notifizierenden Mitgliedstaat explizit dazu, sicherzustellen, dass die Personenidentifizierungsdaten tatsächlich der entsprechenden natürlichen oder juristischen Person zugeordnet sind.[44] Gemäß Art. 11 Abs. 1 eIDAS-VO haftet der Mitgliedstaat für Schäden, die durch eine vorsätzliche oder fahrlässige Verletzung dieser Pflicht entstehen.[45] Dies wird in der Praxis mutmaßlich

---

40 Im Falle von Zwischenstufen kommen die Rechtsfolgen der nächstunteren Stufe zur Anwendung, wenn deren technische Spezifikationen eingehalten werden.

41 Näher Hoffmann 2014: 762 ff.; s.a. im Folgenden.

42 Diese wurden am 8.9.2015 erlassen: Durchführungsverordnung (EU) 2015/1502 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Abs. 3 VO (EU) Nr. 910/2014, Abl. EU Nr. L 235/7 v. 9.9.2015.

43 Der Anhang der Durchführungsverordnung (EU) 2015/1502 (Fn. 42) umfasst elf Seiten mit detaillierten Vorgaben.

44 Zu den übrigen Anforderungen s. Roßnagel 2014: 3688; zur Notifizierbarkeit der deutschen Dienste des elektronischen Identitätsnachweises und der De-Mail s. Hoffmann 2014: 762 ff.

45 Dies ist für das deutsche Recht eine erhebliche Neuerung, weil die Haftungsfragen im Zusammenhang mit dem elektronischen Identitätsnachweis des neuen Perso-

zu einem sehr sorgfältigen Vorgehen der nach nationalem Recht zuständigen Stellen führen.

3.2 Verifikation von Identitäten

Wenn Mitgliedstaaten Identitäten erzeugen, stellt sich die Frage, ob die anderen Mitgliedstaaten diese anerkennen müssen. Dieses Problem tritt für Pässe und Personalausweise (als Reisedokumente) innerhalb der Europäischen Union schon seit langem nicht mehr auf, da diese ohnehin weltweit standardisiert sind.

Für elektronische Signaturen harmonisiert die geltende Signaturrichtlinie die Verwendung innerhalb der Union. Ihr Art. 4 statuiert Binnenmarktgrundsätze und verbietet es den Mitgliedstaaten, die Bereitstellung von Zertifizierungsdiensten aus anderen Mitgliedstaaten und den freien Verkehr von entsprechenden Produkten einzuschränken. § 23 SigG setzt dies in Deutschland um.[46]

Art. 4 eIDAS-VO statuiert entsprechende Binnenmarktgrundsätze für Vertrauensdienste. Völlig neu ist demgegenüber das System der gegenseitigen Anerkennung für elektronische Identifizierungssysteme in Art. 6 eIDAS-VO.[47] Die Vorschrift verpflichtet die Mitgliedstaaten, deren öffentliche Stellen für den Zugang zu Online-Diensten elektronische Identifizierungsmittel verwenden, nach Art. 7 und Art. 9 eIDAS-VO notifizierte Identifizierungsmittel anderer Mitgliedstaaten anzuerkennen. Demgegenüber statuiert die Verordnung keine Pflicht der Mitgliedstaaten, überhaupt elektronische Identifizierungsmittel einzuführen. Theoretisch besteht für die Mitgliedstaaten auch keine Pflicht, elektronische Identifizierungsmittel anderer Staaten anzuerkennen, selbst wenn diese notifiziert sind – dies ist allerdings nur um den (unrealistischen) Preis möglich, auch innerstaatlich auf den Einsatz derartiger eigener Mittel zu verzichten.

Die Vorgabe der gegenseitigen Anerkennung führt unmittelbar zu der Frage der technischen Sicherheit. Der Entwurf der Kommission hatte auf Sicherheitsanforderungen völlig verzichtet und war hierfür vielfach kriti-

---

nalausweises bisher nicht geregelt sind; s. dazu Borges 2011 sowie Möller 2011: Rn. 37 ff.

46 S. näher Roßnagel 2013c: Rn. 19 ff.

47 Ähnlich besteht nach Art. 25 Abs. 3, Art. 35 Abs. 3 und Art. 41 Abs. 3 eIDAS-VO eine Anerkennungspflicht für qualifizierte Signaturen, Siegel und Zeitstempel.

siert worden.[48] Nunmehr sieht Art. 6 Abs. 1 lit. b eIDAS-VO ein System abgestufter Sicherheit vor. Ein Mitgliedstaat kann für das jeweilige Verwaltungsverfahren ein bestimmtes Sicherheitsniveau („niedrig", „substantiell" oder „hoch")[49] vorsehen und muss dann nur solche elektronische Identifizierungssysteme anderer Mitgliedstaaten anerkennen, die dasselbe oder ein höheres Sicherheitsniveau aufweisen.

Die Verordnung enthält auch Mitwirkungspflichten der ausgebenden Mitgliedstaaten hinsichtlich der Verifikation. Gemäß Art. 7 lit. f eIDAS-VO stellt der notifizierende Mitgliedstaat sicher, dass eine Online-Authentifizierung zur Verfügung steht, sodass jeder im Hoheitsgebiet eines anderen Mitgliedstaats niedergelassene vertrauende Beteiligte die in elektronischer Form empfangenen Personenidentifizierungsdaten bestätigen kann.

3.3 Regulierung von Identitäts-Infrastrukturen

Mit der eIDAS-Verordnung hat die Europäische Union nunmehr verbindliche Vorgaben für mehrere Identitäts-Infrastrukturen gemacht. Neben elektronischen Identifizierungsmitteln und elektronischen Signaturen werden weitere Funktionalitäten wie elektronische Siegel (Signaturen für juristische Personen), elektronische Zeitstempel, elektronische Dokumente, Dienste für die Zustellung elektronischer Einschreiben und Zertifizierungsdienste für die Webseiten-Authentifizierung europaweit verbindlich geregelt.[50] Durch den Wechsel des Regulierungsinstruments von der Richtlinie (für elektronische Signaturen) zur Verordnung ergeben sich weitreichende Änderungen zumindest für die Mitgliedstaaten, die wie Deutschland sehr detaillierte nationale Gesetze zur Umsetzung verabschiedet hatten. Freilich lässt die eIDAS-Verordnung trotz ihres gegenüber der Signaturrichtlinie erheblich größeren Detaillierungsgrades viele Fragen offen.

---

48 Z.B. Hornung 2012a: 634; Dumortier und Vandezande 2012: 570; Sädtler 2013: 127; Roßnagel und Johannes 2013: 68; Spindler und Rockenbauch 2013: 142 f.

49 S.o. 3.1.

50 S. Roßnagel 2014: 3686, 3690 f.

3.3.1 Europäische Vorgaben zur Interoperabilität

Da die eIDAS-Verordnung nach Erwägungsgrund 12 „keinen Eingriff in die in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme und zugehörigen Infrastrukturen“ vornehmen will, besteht die größte Herausforderung in der Herstellung von Interoperabilität.[51] Zur Lösung dieses Problems sind durch Forschungsprojekte[52] und die Zusammenarbeit der Behörden der Mitgliedstaaten verschiedene technische Ansätze entwickelt worden, die nicht nur nachgelagerte Umsetzungsfragen betreffen, sondern sich auch mit Blick auf die datenschutzrechtliche Problematik erheblich unterscheiden.[53] Bemerkenswerterweise verrechtlicht der europäische Gesetzgeber nunmehr einige dieser Konzepte und nimmt in Erwägungsgrund 16 explizit auf sie Bezug.[54]

Die notifizierten elektronischen Identifizierungssysteme müssen gemäß Art. 12 Abs. 1 eIDAS-VO interoperabel sein. Zu diesem Zweck wird ein „Interoperabilitätsrahmen“ (Abs. 2) nach bestimmten Kriterien (Abs. 3 und 4) geschaffen: Technologieneutralität, Einhaltung europäischer und internationaler Normen, Förderung von privacy by design sowie Datenverarbeitung im Einklang mit der europäischen Datenschutzrichtlinie. Die Mitgliedstaaten werden in erheblichem Umfang zur Zusammenarbeit verpflichtet (Abs. 5 und 6). Die Kommission hat in Abs. 7 und 8 Befugnisse erhalten, im Wege von Durchführungsrechtsakten sowohl die Zusammenarbeit der Mitgliedstaaten als auch den Interoperabilitätsrahmen näher aus-

---

51 Dabei handelt es sich um ein allgemeines Infrastrukturproblem. Dieses ist in der Union erkannt worden und soll u.a. mit der „Einrichtung eines Programms für Interoperabilitätslösungen und gemeinsame Rahmen für europäische öffentliche Verwaltungen, Unternehmen und Bürger (Programm ISA^2) als Mittel zur Modernisierung des öffentlichen Sektors“ adressiert werden, s. den entsprechenden Beschluss (EU) 2015/2240 v. 25.11.2015, ABl. EU Nr. L 318/1 v. 4.12.2015.

52 Insbesondere das Projekt STORK („Secure idenTity acrOss boRders linked“, s. https://www.eid-stork.eu/).

53 S. den Beitrag von Bender in diesem Band.

54 „Insbesondere das Großpilotprojekt STORK und die ISO-Norm 29115 beziehen sich unter anderem auf die Niveaus 2, 3 und 4, die so weit wie möglich bei der Festlegung technischer Mindestanforderungen, Normen und Verfahren für die Sicherheitsniveaus „niedrig“, „substanziell“ und „hoch“ im Sinne dieser Verordnung berücksichtigt werden sollten, wobei die kohärente Anwendung dieser Verordnung – insbesondere hinsichtlich des Sicherheitsniveaus „hoch“ in Bezug auf den Identitätsnachweis für die Ausstellung qualifizierter Zertifikate – sichergestellt werden sollte.“.

zugestalten – ein weiteres Beispiel für die Europäisierung durch delegierte Rechtsetzung.

Für die Zusammenarbeit hat die Kommission inzwischen ein relativ elaboriertes Verfahren der „gegenseitigen Begutachtung" der nationalen elektronischen Identifizierungssysteme vorgegeben (Art. 7 bis 11 des Durchführungsbeschlusses (EU) 2015/296).[55] Das zugleich eingerichtete „Kooperationsnetz" besteht gemäß Art. 15 aus den Mitgliedstaaten und den Ländern des EWR und arbeitet nach Art. 16 Abs. 1 unter dem Vorsitz der Kommission. Die eigentliche gegenseitige Begutachtung bleibt den Mitgliedstaaten vorbehalten. Allerdings erhalten die Teilnehmer des Kooperationsnetzes nach Art. 8 des Durchführungsbeschlusses eine Reihe von Informationen und gemäß Art. 11 einen Ergebnisbericht über die Begutachtung.

Eine Zusammenarbeit mit Dritten (insbesondere Staaten außerhalb der Union und des EWR) ist in Art. 15 Abs. 3 des Durchführungsbeschlusses nur angedeutet. Danach kann das Kooperationsnetzwerk Experten einladen und Personen oder Organisationen einen Beobachterstatus verleihen.

Die Durchführungsverordnung (EU) 2015/1501 spezifiziert im Detail den Interoperabilitätsrahmen für elektronische Identifizierungssysteme.[56] Dazu werden „Knoten" vorgegeben. Dies sind Anschlusspunkte, die als Teil der Interoperabilitätsarchitektur für die elektronische Identifizierung an der grenzüberschreitenden Authentifizierung von Personen mitwirken und die Datenübertragungen erkennen und verarbeiten oder an andere Knoten weiterleiten können (Art. 2 Nr. 1 der Durchführungsverordnung). So sollen Schnittstellen für die Verbindung zwischen den nationalen elektronischen Identifizierungsinfrastrukturen der Mitgliedstaaten geschaffen werden. Art. 6 Abs. 1 gibt vor, dass der Schutz der Privatsphäre und der Vertraulichkeit der ausgetauschten Daten sowie die Erhaltung ihrer Unversehrtheit zwischen den Knoten „durch den Einsatz der besten verfügbaren technischen Lösungen und Schutzverfahren sichergestellt" werden. Insgesamt ist die Regelung darauf angelegt, keine konkrete technische Archi-

55 Durchführungsbeschluss (EU) 2015/296 v. 24.2.2015 zur Festlegung von Verfahrensmodalitäten für die Zusammenarbeit zwischen den Mitgliedstaaten auf dem Gebiet der elektronischen Identifizierung gemäß Artikel 12 Absatz 7 der Verordnung (EU) Nr. 910/2014, ABl. EU Nr. L 53/14 v. 25.2.2015.

56 Durchführungsverordnung (EU) 2015/1501 v. 8.9.2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014, ABl. EU Nr. L 235/1 v. 9.9.2015.

tektur vorzugeben, sondern nur Gestaltungsprinzipien. Im Grundsatz sind damit beide derzeit diskutierte Umsetzungsstrategien („Proxy“ und „Middleware“)[57] zulässig.

Art. 9 Abs. 3 der Durchführungsverordnung gibt demgegenüber eine problematische Speicherung durch die Knotenbetreiber vor. Diese müssen Daten speichern, mit denen im Falle eines „Vorfalls“ (dieser Begriff ist völlig vage und wird nicht näher spezifiziert) die Abfolge des Meldungsaustauschs rekonstruiert werden kann, damit Ort und Art des Vorfalls festgestellt werden können. Die Daten werden für einen Zeitraum gespeichert, „der im Einklang mit nationalen Vorgaben steht“. Speicherpflichtig sind die Kennung des Knotens, die Kennung der Meldung sowie Datum und Uhrzeit der Meldung. Da die Mitgliedstaaten weitere Daten hinzufügen können, besteht zumindest das Risiko, dass – anders als beim deutschen elektronischen Identitätsnachweis des neuen Personalausweises[58] – Intermediäre als Knoten eingeschaltet werden, die umfassende Transaktionsprotokolle speichern. Dies ist datenschutzrechtlich grundsätzlich abzulehnen, weil so umfassende Kommunikationsprofile entstehen können.[59]

Auch zu einem weiteren datenschutzfreundlichen Merkmal des elektronischen Identitätsnachweises findet sich in der Durchführungsverordnung (EU) 2015/1501 auf den ersten Blick keine Regelung. Dieser ermöglicht mit dem dienste- und kartenspezifischen Kennzeichen nach § 2 Abs. 5 PAuswG die Verwendung eines Pseudonyms, das die eindeutige, aber datenschutzfreundliche Wiedererkennung des Ausweisinhabers zulässt. Zu diesen und anderen Ansätzen des privacy by design enthält die Durchführungsverordnung nur Andeutungen. Stattdessen definiert sie einen „Mindestsatz von Personenidentifizierungsdaten, die eine natürliche oder juristische Person eindeutig repräsentieren“. Dessen Verwendung wird zwar nicht explizit vorgegeben. Wird er jedoch verwendet, so verpflichtet Art. 11 der Durchführungsverordnung dazu, die Anforderungen des Anhangs einzuhalten. Dieser gibt unter anderen die Verwendung einer eindeutigen Kennung vor, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüber-

---

57 S. den Beitrag von Bender in diesem Band.

58 Zur datenschutzrechtlich positiven Bewertung s. die Nachweise in Fn. 14 sowie Möller 2012: 77 ff.

59 S. Hornung, 2015b: 206 ff.; zu Lösungsstrategien der Einbindung von Intermediären („Identitäts-Broker“) s. die Ergebnisse des BMBF-Projekts SkIDentity in Kubach und Hühnlein 2014 sowie Hornung 2012c: 106 f.

schreitenden Identifizierung erstellt wurde und „möglichst dauerhaft fortbesteht“. Dieses „möglichst“ dürfte so zu interpretieren sein, dass die in vielen Mitgliedstaaten zulässigen allgemeinen und dauerhaften Personenkennziffern auch für die elektronische Identifizierungssysteme verwendet werden können, aber keine Pflicht der Mitgliedstaaten besteht, eine solche Ziffer einzuführen.

Bei genauerer Analyse zeigt sich auch, dass die genannte Formulierung dienste- und kartenspezifischen Kennzeichen gemäß § 2 Abs. 5 PAuswG zulässt. Dieses ist nämlich eine „eindeutige Kennung, die vom übermittelnden Mitgliedstaat entsprechend den technischen Spezifikationen für die Zwecke der grenzüberschreitenden Identifizierung erstellt wurde und möglichst dauerhaft fortbesteht“. Unbefriedigend bleibt, dass derartige datenschutzfreundliche Lösungen nur mittels erheblicher Detailkenntnis überhaupt in den Durchführungsverordnungen auffindbar sind. Mit der Vorgabe in Art. 12 Abs. 3 lit. c eIDAS-VO, wonach der Interoperabilitätsrahmen den Grundsatz des privacy by design fördern muss, ist das schwer in Einklang zu bringen.

3.3.2 Querschnittseffekte und verbleibende Kompetenzen der Mitgliedstaaten

Die in der eIDAS-Verordnung geregelten Vertrauens- und Identifizierungsdienste können in praktisch allen Lebens- und Rechtsbereichen eingesetzt werden, in denen Menschen rechtserheblich elektronisch miteinander kommunizieren. Es handelt sich damit um eine Querschnittsregulierung, die erhebliche Auswirkungen auf das Recht der Mitgliedstaaten hat – insbesondere im allgemeinen Vertrags-, Verwaltungs- und Prozessrecht.[60] Dies ist unter Kompetenzgesichtspunkten in doppelter Hinsicht problematisch. Zum einen zentralisiert die Verordnung viele der historisch unterschiedlich gewachsenen nationalen rechtlichen Strukturen in diesen Bereichen. Zum anderen ist mit der neuen Verordnung auch eine Verschiebung von der Legislative auf die Exekutive verbunden, weil die neuen Rechtsgrundlagen (wie bei anderen aktuellen Rechtsetzungsverfahren

60 S. Roßnagel 2014: 3686 f.

auch)[61] vielfach nur ausfüllungsbedürftige Rahmensetzungen enthält, deren Konkretisierung der Europäischen Kommission überantwortet wird.[62]

Trotz dieser insgesamt erheblichen europäischen Zentralisierung verbleiben den Mitgliedstaaten substantielle Kompetenzen. Die eIDAS-Verordnung findet zunächst gemäß Art. 2 Abs. 2 keine Anwendung auf die Erbringung von Vertrauensdiensten, die ausschließlich innerhalb geschlossener Systeme aufgrund von nationalem Recht oder von Vereinbarungen zwischen einem bestimmten Kreis von Beteiligten verwendet werden. Dies betrifft insbesondere Dienst- und Betriebsausweise mit entsprechenden Funktionalitäten. Der Einsatz elektronischer Identifizierungsmittel durch Private (als Anbieter oder Nutzer) wird sogar überhaupt nicht adressiert.[63]

In einigen Bereichen eröffnet die eIDAS-Verordnung explizit Regulierungsspielräume für die Mitgliedstaaten. Aber auch im Übrigen wird die deutsche Signaturgesetzgebung (anders als man zunächst annehmen könnte) keineswegs vollständig verdrängt; dies ist insbesondere durch die in vielen Detailbereichen unvollständige Regulierung der Verordnung bedingt.[64] Ob der europäische Gesetzgeber das erklärte Ziel einer verstärkten Harmonisierung letztlich erreicht, muss deshalb abgewartet werden.

Als Verordnung hat die eIDAS-Verordnung gemäß Art. 288 Abs. 2 AEUV allgemeine Geltung, ist in allen ihren Teilen verbindlich und gilt unmittelbar in allen Mitgliedstaaten. Ebenso wie die Signaturrichtlinie untersagt sie diesen jedoch nicht, weitere Identitäts-Infrastrukturen oder Basisdienste des Electronic Government oder Electronic Commerce zu „erfinden"; dies wird in Erwägungsgrund 25 sogar explizit betont.[65] In der Vergangenheit wurde die Europäische Union allerdings dann tätig, wenn ein Bedürfnis nach den entsprechenden Diensten bestand und einzelne

---

61 S. für den insoweit problematischen Entwurf der Kommission zur europäischen Datenschutzreform Hornung 2012b: 104 ff.; in der verabschiedeten Fassung wurde dies bis auf wenige Fälle gestrichen.

62 Kritisch für die eIDAS-Verordnung Roßnagel und Johannes 2013: 67 f.; Spindler und Rockenbauch 2013: 143 f.; Roßnagel 2014: 3687.

63 Zum insoweit noch undeutlichen Entwurf s. Sädtler 2013: 121; zu den Auswirkungen auf die Privatwirtschaft s. Sosna 2014: 828.

64 S. Roßnagel 2014: 3691 f.; ders. 2015.

65 „Den Mitgliedstaaten sollte es freistehen, auch andere Arten von Vertrauensdiensten zusätzlich zu jenen festzulegen, die auf der in dieser Verordnung vorgesehenen abschließenden Liste der Vertrauensdienste stehen, um diese auf nationaler Ebene als qualifizierte Vertrauensdienste anzuerkennen.".

Mitgliedstaaten gesetzliche Regelungen verabschiedeten, ohne von sich aus übereinstimmende Standards anzustreben oder zu erreichen. Dies war bereits bei der elektronischen Signatur der Fall, für die beispielsweise Deutschland schon im Jahre 1997 gesetzliche Regelungen verabschiedet hatte, bevor im Jahre 1999 die Signaturrichtlinie folgte. Die Regelungen der eIDAS-Verordnung zur elektronischen Identifizierung sind in vergleichbarer Weise eine Reaktion auf die sehr heterogene Landschaft, die die verschiedenen Aktivitäten der Mitgliedstaaten zur Bereitstellung elektronischer Identitäten für ihre Bürger hervorgebracht hat.

3.3.3 Verhältnis zu Drittstaaten

Art. 14 eIDAS-VO bestimmt eine Gleichstellung der Angebote von Vertrauensdienstleistern aus Drittländern mit den in der Union niedergelassenen Dienstleistern, wenn die Vertrauensdienste aus dem Drittland im Rahmen einer gemäß Art. 218 AEUV geschlossenen Vereinbarung zwischen der Union und dem betreffenden Drittland oder einer internationalen Organisation anerkannt sind.

Dagegen enthält die eIDAS-Verordnung keinerlei Regelung zu Identifizierungssystemen aus Drittstaaten.[66] Das Kooperationsnetz nach Art. 15 des Durchführungsbeschlusses (EU) 2015/296[67] lässt einen begrenzten Informationsaustausch mit den Staaten des Europäischen Wirtschaftsraums und weiteren Staaten (als Beobachter) zu. Eine Begutachtung und Anerkennung elektronischer Identifizierungssysteme von Staaten jenseits der Union sind jedoch nicht vorgesehen.

Hintergrund ist mutmaßlich die unterschiedliche Struktur der geregelten Anbieter: Während Vertrauensdienste nach der Systematik der eIDAS-Verordnung privatwirtschaftlich angeboten werden, wird die Notifizierung elektronischer Identifizierungssysteme gemäß Art. 7 lit. a eIDAS-VO nur für solche Systeme geregelt, die vom notifizierenden Mitgliedstaat oder in seinem Auftrag ausgestellt oder zumindest von ihm anerkannt werden. Es besteht also ein viel stärkerer Bezug zu dem jeweils national bestimmten Verhältnis des Staates zu seinen Bürgern als bei Vertrauensdiensten. Dies würde bei einer rechtlichen Anerkennung über die Union hinaus vermut-

66 Kritisch Spindler und Rockenbauch 2013: 147.
67 S.o. 3.3.1.

lich zu Problemen führen, etwa bei der in Art. 11 eIDAS-Verordnung statuierten Haftung der notifizierenden Mitgliedstaaten für Identifizierungsfehler.

Trotz dieser Schwierigkeiten wäre es mit Blick auf die weltweiten Entwicklungen und Probleme[68] sinnvoll gewesen, zumindest die grundsätzliche Möglichkeit der rechtlichen Anerkennung elektronischer Identifizierungssysteme jenseits der Union vorzusehen und einen entsprechenden institutionalisierten Austausch zu ermöglichen. Im weltweiten „Wettbewerb" um die effektivste Regulierung des elektronischen Identitätsmanagements hätte Europa auf diesem Weg zumindest ein rechtlich strukturiertes Forum etablieren können.

3.4 Datenschutz und Identitätsmanagement

Manche Definitionen von elektronischer Identität oder elektronischem Identitätsmanagement sind so umfassend, dass sie letztlich mehr oder weniger alle personenbezogenen Daten erfassen.[69] Rechtsfragen des elektronischen Identitätsmanagements sind dann gleichbedeutend mit dem Datenschutzrecht.

Auch wenn man einen engeren Begriff des elektronischen Identitätsmanagements wählt, ist freilich eindeutig, dass dieses eng mit dem Datenschutzrecht verknüpft ist. In der spezifisch deutschen Begründung des verfassungsrechtlichen Datenschutzes aus Überlegungen personaler Selbstbestimmung liegt die Verbindung besonders nahe;[70] sie wird aber auch in anderen Staaten (beispielsweise den USA)[71] erkannt. Art. 5 Abs. 1 eIDAS-VO verpflichtet zur datenschutzkonformen Verwendung personenbezogener Daten, und der Interoperabilitätsrahmen muss nach Art. 12 Abs. 3 lit. c eIDAS-VO den Grundsatz des privacy by design fördern. Aufsichtsstellen arbeiten nach Art. 17 Abs. 4 lit. f und Art. 20 Abs. 2 Satz 2 eIDAS-VO mit den Datenschutzbehörden zusammen.

---

68 S.o. 2.2.

69 S. dazu etwa den Beitrag von Schallaböck in diesem Band; Andrade (2011) schlägt vor, Identität als materielles Schutzgut eines prozedural ausgestalteten Datenschutzrechts zu verstehen.

70 Dazu Hornung 2005: 30 ff.

71 S. The White House 2011: 11: das erste der „guiding principles" lautet: „Identity Solutions will be Privacy-Enhancing and Voluntary". Dies wird in dem Dokument vielfach wiederholt und technisch ausgeformt.

3.4.1 Erweiterung der Perspektive

Die datenschutzrechtliche Perspektive stellt in mehrfacher Hinsicht eine erhebliche Erweiterung der rechtlichen Regulierung des elektronischen Identitätsmanagements dar. Erstens geht es nicht um konkrete Identitätsmanagement-Systeme wie ein nationales Ausweisdokument, sondern um allgemeine Anforderungen an dem Umgang mit Identitätsdaten – unabhängig davon, ob diese bei elektronischen Signaturen oder Identifizierungsdiensten, bei staatlichen oder privaten Anbietern,[72] allgemein zugänglich oder in geschlossenen Nutzergruppen wie bei betrieblichen und behördlichen Mitarbeiterausweisen anfallen. Zweitens wird die Perspektive um den weiteren Umgang mit den Daten erweitert und der datenschutzrechtlich Betroffene in den Mittelpunkt gestellt. Der Fokus beschränkt sich nicht auf die Frage der sicheren Erzeugung und Verifikation von Identitäten, sondern richtet sich gerade auf das Problem eines selbstbestimmten Identitätsmanagements. Dieses setzt vielfach Anonymität und Pseudonymität voraus – und damit Nicht-Identifizierbarkeit zumindest in bestimmten Kontexten und gegenüber bestimmten anderen Akteuren.

Schließlich kommt drittens auch begrifflich eine andere Vorstellung von Identität ins Spiel: Elektronisches Identitätsmanagement ist aus dieser Perspektive nicht lediglich ein Identifizierung- und Berechtigungsmanagement, sondern muss in den Kontext verschiedener Dimensionen personaler Identität gestellt werden, weil die umfassende Erhebung und Verwendung personenbezogener Daten insbesondere dann Auswirkungen auf die Persönlichkeitsentfaltung haben kann, wenn diese einseitig, intransparent und umfassend erfolgt. Dies hat das Bundesverfassungsgericht schon im Volkszählungsurteil erkannt und dort betont, dass mit dem Recht auf informationelle Selbstbestimmung eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar wären, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“.[73]

---

72 S.o. 2.2.2.
73 BVerfGE 65, 1 (43).

3.4.2 Identitätsmanagement in der Datenschutzreform

Das europäische Datenschutzrecht befindet sich derzeit im Umbruch. Auf den Vorschlag der Europäischen Kommission am 25. Januar 2012 für eine Datenschutz-Grundverordnung (DS-GVO)[74] folgte eine insbesondere in Deutschland, aber auch darüber hinaus intensiv geführte rechtspolitische Debatte über angemessene Regelungen für die Erhebung und Verwendung personenbezogener Daten in der vernetzten Informationsgesellschaft.[75] Das europäische Parlament hat am 12. März 2014,[76] der Rat am 11. Juni 2015[77] seine Position festgelegt. Im Trilog wurde Mitte Dezember ein Kompromiss erzielt. Die am 27. April 2016 formell beschlossene Verordnung wird nach einer Übergangszeit ab dem 25. Mai 2018 gelten.

Von den vielen und inzwischen intensiv diskutierten Regelungen der Reform können einige für das elektronische Identitätsmanagement besonders relevant werden:[78]

- Art. 4 Nr. 1 DS-GVO behält das Konzept der personenbezogenen Daten bei und stellt auf die direkte oder indirekte Bestimmbarkeit des Betroffenen ab. Dies war schon Inhalt aller Positionen im Trilog.
- Der erweiterte Vorschlag des Berichterstatters des Europäischen Parlaments zum Anwendungsbereich konnte sich in den internen Verhandlungen nicht durchsetzen. Danach sollte es neben der direkten oder indirekten Bestimmbarkeit auch ausreichen, wenn eine Person „herausgegriffen“ („singled out“) werden kann. Dadurch wäre auch das Verwalten stabiler Attribute im Identitätsmanagement erfasst worden, wenn die (genaue) Identität der Betroffenen nicht bekannt ist.
- Auf Vorschlag des Parlaments wird eine Definition des Pseudonyms aufgenommen (Art. 4 Nr. 5 DS-GVO).[79] Dies erfolgt erstmals im

74 KOM(2012) 11 endg.

75 Die Diskussion wird inzwischen umfangreich und in erheblicher Ausdifferenzierung geführt; s. als Zwischenstand zu den Kontroversen Hornung 2013a.

76 P7_TA-PROV(2014)0212.

77 Abrufbar unter http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf; eine Gegenüberstellung ist unter https://www.lda.bayern.de/media/baylda_synopse.pdf verfügbar.

78 S. zum Folgenden (noch ohne die Position des Rats) bereits Hornung 2015b: 201 ff.

79 „Pseudonymisierung" ist danach „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet wer-

europäischen Recht[80] und eröffnet Anknüpfungspunkte für Regelungen zum Identitätsmanagement, weil so auch partielle Identitäten erfasst werden können. Voraussetzung ist freilich, dass es nicht zu einer Privilegierung insbesondere von Webtracking-Anbietern kommt, die nur vorgeblich mit Pseudonymen arbeiten, tatsächlich jedoch einen Personenbezug herstellen können.

- Die (wenigen) Regelungen über den höheren Datenschutz bei Kindern[81] können mit identitätstheoretischen Überlegungen der Identität als psychologischem Veränderungsprozess in Verbindung gebracht werden.
- Das von der Kommission vorgeschlagene „Recht auf Datenübertragbarkeit" (Art. 20 DS-GVO)[82] wurde im Trilog zwar wesentlich eingeschränkt, hinsichtlich der durch die Nutzer bereitgestellten Daten aber beibehalten. Es ist maßgeblich durch die Datenschutzfragen sozialer Netzwerke beeinflusst,[83] wird aber auch andere Dienstleister erfassen,

---

den können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.".

80 In Deutschland gibt eine Definition in § 3 Abs. 6a BDSG. Erste Regelungen enthielten bereits die im Jahre 1997 verabschiedeten § 4 Abs. 1 und 4, § 7 TDDSG sowie § 13 Abs. 1 und 4, § 16 Abs. 1 MDStV.

81 Neben Art. 8 DS-GVO (Festlegung des Einwilligungsalters bei Internetdiensten auf das vollendete 16. Lebensjahr mit der Möglichkeit für die Mitgliedstaaten, dies bis maximal auf das vollendete 13. Lebensjahr herabzusetzen, s. näher Hornung 2014: 123 ff.) sind dies v.a. Vorgaben zu der Abwägung mit berechtigten Interessen (Art. 6 Abs. 1 lit. f), den Transparenzanforderungen (Art. 12 Abs. 1 Satz 1: adressatengerechte Sprache", s.a. EG 58), dem Recht auf Vergessenwerden (Art. 17 Abs. 1 lit. f; EG 65 betont zu Recht das Problem, dass die mit der Verarbeitung verbundenen Gefahren noch nicht in vollem Umfang erkannt werden) und der Risikobewertung (EG 75 nennt die Verarbeitung der Daten von verletzlichen Personen als Beispiel für besonders riskante Verarbeitungsprozesse und hebt hierbei Kinder hervor; daraus resultiert – auch wenn das anders als in den Entwürfen nicht mehr ausdrücklich im Normtext verankert ist – etwa die Pflicht zu einer Datenschutz-Folgenabschätzung nach Art. 33). Überdies müssen die Aufsichtsbehörden Aktivitäten besonders beobachten, die sich direkt an Kinder richten, s. Art. 57 Abs. 1 lit. b.

82 In den Entwürfen Art. 18 Abs. 1 DS-GVO-E (Kommission und Rat) bzw. Art. 15 Abs. 2a (Parlament); s. hierzu Roßnagel und Kroschwald 2014: 498.

83 S.a. den zugehörigen EG 68; s. ferner Kipker und Voskamp 2012: 740 f.; Hornung 2014: 123 ff.

also beispielsweise Cloud-Anwendungen[84] und Identitätsmanagement-Systeme. Dementsprechend werden die Anbieter derartiger Systeme dazu verpflichtet sein, ihren Kunden eine Kopie der verarbeiteten Daten in einem „strukturierten gängigen elektronischen Format" bereitzustellen und sie bei einem Anbieterwechsel nicht zu behindern.

- Das gleichfalls neue – nach neuester Rechtsprechung des Europäischen Gerichtshofs in einer bestimmten Ausprägung auch in der aktuellen Richtlinie enthaltene[85] – „Recht auf Vergessenwerden" ist zwar mit vielen technischen und rechtlichen Problemen behaftet.[86] Die hinter ihm stehenden zutreffenden Überlegungen sind aber gerade die, die auch für ein datenschutzfreundliches, nutzergesteuertes Identitätsmanagement sprechen: Der Einzelne soll nicht sein Leben lang mit Informationen konfrontiert werden, die andere über ihn gesammelt haben – noch dazu, wenn diese Datensammlungen über die Grenzen sozialer Rollen hinweg als Profile zusammengetragen wurden. Auch wenn Art. 17 DS-GVO nunmehr weitgehend dem bisher schon geltenden Recht entspricht, wird dieses grundlegende Problem die Datenschutzpraxis auch in Zukunft erheblich beschäftigen.
- Viel zu wenig Unterstützung erhielt ein datenschutzkonformes Identitätsmanagement im Entwurf der Kommission an einem besonders wichtigen Punkt. Der Vorschlag sprang hinsichtlich des Datenschutzes durch Technik viel zu kurz und erwähnte beispielsweise grundlegende Konzepte wie Anonymität und Pseudonymität noch nicht einmal.[87] Aussagen zur Technikgestaltung fehlten ebenso wie verbindliche Vorgaben für Zertifizierungen und Datenschutzsiegel und -zeichen. Die Position des Parlaments enthielt Verbesserungen.[88] So wurde beispielsweise vorgeschlagen, dass der Datenschutz durch Technik zur Förderung einer breiten Umsetzung in verschiedenen Wirtschaftssektoren eine Voraussetzung für Angebote im Rahmen öffentlicher Ausschrei-

---

84 S. Hornung und Sädtler 2012: 641.

85 S. EuGH, Urteil vom 13.5.2014 – C-131/12 (Google Spain SL u. Google Inc./ Agencia Española de Protección de Datos [AEPD] u. Mario Costeja Conzález), NJW 2014, 2257; der EuGH verwendet den Begriff nicht.

86 S. ausführlich Hornung und Hofmann 2013: 163 ff.; mit unterschiedlich starker Kritik: Costa und Poullet 2012: 256 f.; Jaspers 2012: 572 f.; Koreng und Feldmann 2012: 311; Kort 2012: 1022 f.; Lang 2012: 149; Wybitul und Fladung 2012: 510 f.; Kodde 2013: 115; zu konzeptionellen Überlegung s. Mayer-Schönberger 2009.

87 S. Hornung 2012: 103 f.; s. ferner Münch 2012: 72 ff.; Richter 2012: 576 ff.

88 Art. 23 DS-GVO-E (Rat), s. dazu Hornung 2005: 1 ff.

bungen werden sollte. Dies hat sich leider nicht durchgesetzt, immerhin enthält Art. 25 DS-GVO aber nunmehr deutlich spezifischere Regelungen einschließlich der Prinzipien der Pseudonymisierung und Datensparsamkeit. Auch die Bestimmungen zur Zertifizierung (Art. 42, 43 DS-GVO) wurden erheblich präzisiert.[89] Überdies enthält Art. 21 Abs. 5 DS-GVO auf Vorschlag des Parlaments eine Art „do not track"-Klausel. Danach soll das Recht zum Widerspruch im Internet auch in standardisierter automatisierter Form ausgeübt werden können.

Insgesamt werden die Regelungen der Datenschutz-Grundverordnung in vielen Fällen hinter bereichsspezifische Erhebungs- und Verwendungsregelungen zurücktreten, die der europäische Gesetzgeber in anderen Rechtsakten für einzelne Typen des elektronischen Identitätsmanagements verabschiedet. Gerade in Art. 5 Abs. 1 eIDAS-VO wird jedoch auf die geltende Datenschutzrichtlinie (und künftig auf die Grundverordnung) verwiesen, sodass die erläuterten allgemeinen Regelungen eine erhebliche Bedeutung behalten werden.

4 Ausblick: Regelungsebenen und Akteure

Insgesamt sind die aktuellen europäischen Entwicklungen ein sehr instruktives Beispiel für die Herausforderungen der technischen Implementierung und der rechtlichen Regulierung eines grenzüberschreitenden elektronischen Identitätsmanagements. Technische Interoperabilität, rechtliche Anforderungen des Datenschutzes und der (gerichtsfesten) Beweisbarkeit[90] sowie europäische und nationalstaatliche politische Verständnisse des Verhältnisses von Bürgern und Staat interagieren auf komplexe Weise miteinander.

Es ist deutlich, dass diese Entwicklung nach wie vor am Anfang steht. Ob sich die Vertrauensdienste am Markt etablieren und die Bürger die staatlicherseits angebotenen Identifizierungssysteme annehmen, bleibt abzuwarten und hängt von weiteren Faktoren und Umsetzungsstrategien ab – insbesondere der Etablierung angemessener Finanzierungsmodelle, die die Kosten der jeweiligen Infrastruktur denjenigen zuweisen, die einen ent-

89 S. zur Diskussion um die Zertifizierung nach der Datenschutz-Grundverordnung Hornung und Hartl 2014.

90 Zu der Anforderung der Rechtssicherheit s. Hornung 2015b: 194 ff.

sprechenden Nutzen haben. Nach wie vor fehlt häufig die Erkenntnis, dass es sich bei den Basisdiensten der elektronischen Signatur, Authentisierung und Verschlüsselung weniger um Produkte, sondern um Infrastrukturen handelt, die sich nur begrenzt aufgrund von Marktmechanismen etablieren werden.[91] Elektronisches Identitätsmanagement wird damit Teil der staatlichen Daseinsvorsorge.[92]

Als Herausforderungen für die Zukunft stellen sich die Ausfüllung des nunmehr neuen rechtlichen Rahmens, die Zusammenarbeit über Europa hinaus und die kontinuierliche Entwicklung und Gestaltung datenschutzfreundlicher Technologien eines nutzerzentrierten Identitätsmanagements.[93] Nachdem die Kommission inzwischen tätig geworden ist, müssen nunmehr die Mitgliedstaaten prüfen, welche Umsetzungsakte erforderlich sind. Als weitere Akteure werden über kurz oder lang Gerichte – insbesondere der Europäische Gerichtshof – hinzutreten, die wesentliche Inhalte der offenen Begriffe der Rechtsakte rechtsverbindlich klären müssen.

Mutmaßlich wird Europa hiermit eine Weile beschäftigt sein; dies sollte aber nicht dazu verleiten, die weltweiten, insbesondere transatlantischen Fragen zu ignorieren. Hier wird sich auch das Problem der Interoperabilität noch einmal neu stellen. Es bleibt zu hoffen, dass diese stärker als bisher als zwar notwendiges, nicht aber hinreichendes Kriterium der Einführung elektronischer Identitätsmanagementsystemen begriffen wird. Nicht nur aus rechtlichen, sondern auch aus Akzeptanzgründen ist daran festzuhalten, dass diese Systeme den Nutzer und seine informationelle Selbstbestimmung in den Mittelpunkt stellen müssen.

---

91 S. Roßnagel 2013a: 2710 f., 2716; zu den damit verbundenen Verbreitungsproblemen der qualifizierten elektronischen Signatur s. Roßnagel 2013b: Rn. 138 ff.; mit Blick auf die eIDAS-Verordnung auch Roßnagel und Johannes 2013: 72; s.a. Hornung 2015b: 204 ff.

92 Dazu ausführlich Luch und Schulz 2010.

93 S. zu den Anforderungen an ein solches System z.B. Hansen et al. 2005; viele Einzelfragen wurden in den EU-Projekten PRIME (https://www.prime-project.eu/), PrimeLife (http://primelife.ercim.eu/), FIDIS (http://www.fidis.net/) und ABC4Trust (https://abc4trust.eu/) untersucht; zu den Ergebnissen s. z.B. Camenisch et al. 2011.

Literatur

Altmann, Mareike (2010): *Freiheitsbeschränkung durch den Reisepass? Die Vereinbarkeit der EG VO 2252/2004 mit Grund- und Menschenrechten*, Baden-Baden: Nomos.

Andrade, Norberto Nuno Gomes de (2011): „Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights", in: Fischer-Hübner Simone, Duquenoy Penny, Hansen Marit, Leenes, Roland and Zhang Ge (Eds.), *Privacy and Identity Management for Life*, IFIP AICT 352, 90-107.

Andrade, Norberto Nuno Gomes de (2012): „Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID", in: *Computer Law and Security Review* 28(2), 153-162.

Baier, Tobias (2006): *Persönliches digitales Identitätsmanagement. Untersuchung und Entwicklung von Konzepten und Systemarchitekturen für die kontrollierte Selbstdarstellung in digitalen Netzen*, http://ediss.sub.uni-hamburg.de/volltexte/2006/2746/pdf/TBaier-Diss-IDM.pdf.

Bogdanowicz, Mark und *Beslay, Laurent* (2001): „Cybersicherheit und die Zukunft der Identität", in: *The IPTS Report* 57, 31-39.

Borges, Georg (2010): „Der neue Personalausweis und der elektronische Identitätsnachweis", in: *Neue Juristische Wochenschrift* 63(46), 3334-3339.

Borges, Georg (2011): *Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis*, Baden-Baden: Nomos.

Camenisch Jan, Fischer-Hübner Simone and *Rannenberg Kai (Eds.)* (2011): *Privacy and Identity Management for Life*, Berlin-Heidelberg: Springer.

Costa, Luiz and Poullet, Yves (2012): „Privacy and the regulation of 2012", in: *Computer Law and Security Report* 28(3), 254-262.

Dumortier, Jos and *Vandezande, Niels* (2012): „Trust in the proposed EU regulation on trust services?", in: *Computer Law and Security Review* 28(5), 568–576.

Engemann, Christoph (2012): „Write me down, make me real – zur Gouvernemedialität digitaler Identität", in: Passoth, Jan-H. und Wehner, Josef (Hrsg.), *Quoten, Kurven und Profile: Zur Vermessung der sozialen Welt*, Wiesbaden: VS Verlag für Sozialwissenschaften, 205-227.

Engemann, Christoph (2015): „Die Adresse des freien Bürgers: Digitale Identitätssysteme Deutschlands und der USA im Vergleich", in: *Leviathan* 43(1), 43-63.

Groebner, Valentin (2004): *Der Schein der Person. Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters*, München: C.H. Beck.

Hailbronner, Kai (2010): „Staatsangehörigkeit und Völkerrecht", in: Hailbronner Kay, Renner Günter, Wiedemann Marianne und Maaßen Hans-Georg, *Staatsangehörigkeitsrecht*, 5. Auflage, München: C.H.Beck, 59-124.

Hansen Marit, Borcea-Pfitzmann Katrin und *Pfitzmann Andreas* (2005): „PRIME – Ein europäisches Projekt für nutzerbestimmtes Identitätsmanagement", in: *Information Technology* 47(6), 352-359.

Hoffmann, Christian (2014): „EU-Verordnung über elektronische Identifizierung auf nationale Angebote. Auswirkungen auf De-Mail, E-Postbrief und nPA“, in: *Datenschutz und Datensicherheit* 38(11), 762-767.

Hornung, Gerrit (2005): *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren*, Baden-Baden: Nomos.

Hornung, Gerrit (2011): „Einführung“, in: Hornung, Gerrit und Möller, Jan, *Passgesetz-Personalausweisgesetz: PassG/PAuswG*, München: C.H. Beck, 1-26.

Hornung, Gerrit (2012a): „Brüsseler Angriff auf den neuen Personalausweis?“, in: *Multimedia und Recht* 15(10), 633-634.

Hornung, Gerrit (2012b): „Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012“, in: *Zeitschrift für Datenschutz* 2(3), 99-106.

Hornung, Gerrit (2012c): „Der Einsatz des neuen Personalausweises in Cloud-Anwendungen der kommunalen Verwaltung: Chancen und rechtliche Grenzen“, in: v. Lucke Jörn, Geiger Christian P., Kaiser Siegfried, Schweighofer Erich und Wimmer Maria A. (Hrsg.), *Staat und Verwaltung auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur,* Friedrichshafen: Zeppelin Universität Friedrichshafen, 103-108.

Hornung, Gerrit (2013a): „Die europäische Datenschutzreform – Stand, Kontroversen und weitere Entwicklung“, in: Scholz, Matthias und Funk, Axel (Hrsg.), *DGRI Jahrbuch 2012*, Köln: Otto Schmid, 1-24.

Hornung, Gerrit (2013b): „§ 3 SigV: Identitätsprüfung und Attributsnachweise“, in: Roßnagel, Alexander (Hrsg.), *Beck'scher Kommentar zum Recht der Telemedien-dienste*, München: C.H. Beck, 841-848.

Hornung, Gerrit (2014): „Europa und darüber hinaus. Konzepte für eine Neuregelung des Datenschutzes im Internet und in sozialen Netzwerken“, in: Hill, Hermann und Schliesky, Utz (Hrsg.), *Die Neubestimmung der Privatheit*, Baden-Baden: Nomos, 123-152.

Hornung Gerrit (2015a): „Datenschutzrechtliche Aspekte der Social Media“, in: Hornung, Gerrit und Müller-Terpitz, Ralf (Hrsg.), *Rechtshandbuch Social Media*, Berlin/Heidelberg: Springer, 79-130.

Hornung, Gerrit (2015b): „Zwischen Rechtssicherheit und Persönlichkeitsschutz: Rechtsfragen des Identitätsmanagements im Cloud Computing“, in: Roßnagel, Alexander (Hrsg.), *Wolken über dem Rechtsstaat? Recht und Technik des Cloud Computing in Verwaltung und Wirtschaft*, Baden-Baden: Nomos, 189-216.

Hornung, Gerrit und Hartl, Korbinian (2014): „Datenschutz durch Marktanreize – auch in Europa? Stand der Diskussion zu Datenschutzzertifizierung und –audit", in: *Zeitschrift für Datenschutz* 4(5), 219-225.

Hornung, Gerrit und *Hofmann, Kai* (2013): „Ein ‚Recht auf Vergessenwerden‘? Anspruch und Wirklichkeit eines neuen Datenschutzrechts“, in: *Juristenzeitung* 68(4), 163-170.

Hornung Gerrit und *Sädtler Stephan* (2012): „Europas Wolken. Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing", in: *Computer & Recht* 28(10), 638-645.

Hühnlein, Detlef (2008): „Identitätsmanagement. Eine visualisierte Begriffsbestimmung", in: *Datenschutz und Datensicherheit* 32(3), 163-165.

ISO/IEC JTC 1/SC 27/WG 5 (2007): *Identity management and privacy technologies*, https://www.itu.int/dms_pub/itu-t/oth/06/0D/T060D0000010011PDFE.pdf.

Jandt, Silke (2015): „Beweissicherheit im elektronischen Rechtsverkehr. Folgen der europäischen Harmonisierung", in: *Neue Juristische Wochenschrift* 68(17), 1205-1211.

Jaspers, Andreas (2012): „Die EU-Datenschutz-Grundverordnung. Auswirkungen der EU-Datenschutz-Grundverordnung auf die Datenschutzorganisation des Unternehmens", *Datenschutz und Datensicherheit* 36(8), 571-575.

Kipker, Dennis-Kenji und *Voskamp, Friederike* (2012): „Datenschutz in sozialen Netzwerken nach der Datenschutzgrundverordnung", in: *Datenschutz und Datensicherheit* 36(10), 737-742.

Knight, Alison and *Saxby, Steve* (2014): „Identity crisis: Global challenges of identity protection in a networked world", in: *Computer Law and Security Review* 30(6), 617-632.

Kodde, Claudia (2013): „Die ‚Pflicht zu Vergessen'. ‚Recht auf Vergessenwerden' und Löschung in BDSG und DS-GVO", in: *Zeitschrift für Datenschutz* 3(3), 115-118.

Koreng, Ansgar und *Feldmann, Thorsten* (2012): „Das ‚Recht auf Vergessen'. Überlegungen zum Konflikt zwischen Datenschutz und Meinungsfreiheit", in: *Zeitschrift für Datenschutz* 2(7), 311-315.

Kort, Michael (2012): „Datenschutzrecht in der Europäischen Union: de lege lata und de lege ferenda", in: *Der Betrieb* 65(18), 1020-1024.

Kubach, Michael und *Hühnlein, Detlef* (Hrsg.) (2014): *Vertrauenswürdige Identitäten für die Cloud*, Stuttgart: Fraunhofer Verlag.

Kubicek, Herbert und *Noack, Torsten* (2010): *Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich*, Berlin u.a.: LIT Verlag.

Lang, Markus (2012): „Reform des EU-Datenschutzrechts", in: *Kommunikation und Recht* 15(3), 145-151.

Lehnert, Matthias (2014): *Frontex und operative Maßnahmen an den europäischen Außengrenzen, Verwaltungskooperation. Materielle Rechtsgrundlagen, institutionelle Kontrolle,* Baden-Baden: Nomos.

Luch, Anika und *Schulz, Sönke E.* (2010): „Aktuelle Bedeutung des Identitätsmanagements: Authentisierung, sichere Kommunikation und Dokumentensafes als Elemente einer elektronischen Grundversorgung", in: Schliesky Utz (Hrsg.), *Technikgestütztes Identitätsmanagement. Rechtsfrage und Lösungsvorschläge: dargestellt am Beispiel der De-Mail und elektronischer Dokumentensafes,* Kiel: Lorenz-von-Stein-Institut, 1-21.

Mayer-Schönberger, Viktor (2009): *Delete: The Virtue of Forgetting in the Digital Age*, New Jersey: Princeton University Press.

Mims, Christopher, *How OpenID Lost to Facebook Connect in the Battle for Your Online Identity*, http://www.technologyreview.com/view/421872/how-openid-lost-to-facebook-connect-in-the-battle-for-your-online-identity/.

Moser-Knierim, Antonie (2013): „'Facebook-Login' – datenschutzkonformer Einsatz möglich? Einsatz von Social Plug-ins bei Authentifizierungsdiensten", in: *Zeitschrift für Datenschutz* 3(6), 263-266.

Möller, Jan (2011): „§ 18 PAuswG: Elektronischer Identitätsnachweis", in: Hornung, Gerrit und Möller, Jan, *Passgesetz-Personalausweisgesetz: PassG/PAuswG*, München: C.H. Beck, 234-248.

Möller, Jan (2012): „Informationelle Selbstbestimmung mit dem elektronischen Identitätsnachweis", in: Peters Falk, Kersten Heinrich und Wolfenstetter Klaus-Dieter (Hrsg.), *Innovativer Datenschutz,* Berlin: Duncker & Humblot, 77-90.

Münch, Peter (2012): „Lässt der Entwurf der Entwurf einer Europäischen-Datenschutzgrundverordnung eine Modernisierung des technisch-organisatorischen Datenschutzes erwarten?", in: *Recht der Datenverarbeitung* 28(2), 72-77.

Pallasky, Ansgar (2007): *Datenschutz in Zeiten globaler Mobilität. Eine Untersuchung des Verhältnisses von Datenschutz und Gefahrenabwehr im Reisebereich*, Baden-Baden: Nomos.

Pfitzmann, Andreas and *Hansen, Marit* (2010): *A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management,* http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v 0.34.pdf.

Polenz, Sven (2010): „Der neue elektronische Personalausweis. E-Government im Scheckkartenformat", in: *Multimedia und Recht* 13(10), 671-676.

Quiring-Kock, Gisela (2013): „Entwurf EU-Verordnung über elektronische Identifizierung und Vertrauensdienste", in: *Datenschutz und Datensicherheit* 37(1), 20-24.

Richter, Philipp (2012): „Datenschutz durch Technik und die Grundverordnung der EU-Kommission", *Datenschutz und Datensicherheit* 36(8), 576-580.

Rosner, Gilad L. (2014): *Identity management policy and unlinkability: a comparative case study of the US and Germany,* Univ. Nottingham, PhD thesis, http://eprints.nottingham.ac.uk/14358/1/Full_Draft_v 4.1.4.2_FINAL_post-viva_corrections.pdf.

Roßnagel, Alexander (2013a): „Auf dem Weg zur elektronischen Verwaltung – Das E-Government-Gesetz", in: *Neue Juristische Wochenschrift* 66(37), 2710-2716.

*Roßnagel, Alexander (*2013b): „Einleitung SigG", in: ders. (Hrsg.), *Beck'scher Kommentar zum Recht der Telemediendienste*, München: C.H. Beck, 423-461.

Roßnagel, Alexander (2013c): „§ 23 SigG", in: ders. (Hrsg.), *Beck'scher Kommentar zum Recht der Telemediendienste*, München: C.H. Beck, 776-790.

Roßnagel, Alexander (2014): „Neue Regeln für sichere elektronische Transaktionen. Die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste", in: *Neue Juristische Wochenschrift* 67(51), 3686-3692.

Roßnagel, Alexander (2015): „Der Anwendungsvorrang der eIDAS-Verordnung. Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar?", in: *Multimedia und Recht* 18(6), 359-364.

Roßnagel, Alexander und *Hornung, Gerrit* (2005): „Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck – Die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“, in: *Die Öffentliche Verwaltung* 58(23), 983-989.

Roßnagel, Alexander und *Hornung, Gerrit* (2009): „Ein Ausweis für das Internet – Der neue Personalausweis erhält einen ‚elektronischen Identitätsnachweis‘“, in: *Die Öffentliche Verwaltung* 62(8), 301-305.

Roßnagel Alexander, Hornung Gerrit und Schnabel Christoph (2008): „Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht“, in: *Datenschutz und Datensicherheit* 32(3), 168-172.

Roßnagel, Alexander und *Johannes, Paul C.* (2013): „Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – Neue Regeln für elektronische Sicherheitsdienste“, in: *Zeitschrift für Datenschutz* 3(2), 65-72.

Roßnagel, Alexander und *Kroschwald, Steffen* (2014): „Was wird aus der Datenschutzgrundverordnung? – Die Entschließung des Europäischen Parlaments über ein Verhandlungsdokument“, in: *Zeitschrift für Datenschutz* 4(10), 495-500.

Sädtler, Stephan (2013): „Identity management in cloud computing in conformity with European law? – Problems and approaches pursuant the proposal for a regulation by the European Commission on electronic identification and trust services for electronic transactions in the internal market“, in: Hühnlein, Detlef und Roßnagel, Heiko (Hrsg.), *Open Identity Summit 2013*, Lecture Notes in Informatics (LNI), Bonn: Gesellschaft für Informatik (GI), 118-129.

Schäffer, Heiko (2007): *Der Schutz des zivilen Luftverkehrs vor Terrorismus. Der Beitrag der International Civil Aviation Organization (ICAO)*, Baden-Baden: Nomos.

Schnabel, Christoph und *Freund, Bernhard* (2010): „‘ach wie gut, dass niemand weiß ...‘ – Selbstdatenschutz bei der Nutzung von Telemedienangeboten“, in: *Computer und Recht* 26(11), 718-721.

Schroeder, Werner und *Obwexer, Walter* (Hrsg.) (2015): *20 Jahre Unionsbürgerschaft. Konzept, Inhalt und Weiterentwicklung des grundlegenden Status der Unionsbürger. EuR-Beiheft 1/2015*, Baden-Baden: Nomos.

Schulz, Sönke E (2009): „Der neue ‚E-Personalausweis‘ – elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement“, in: *Computer und Recht* 25(4), 267-272.

Sosna, Sabine (2014): „EU-weite elektronische Identifizierung und Nutzung von Vertrauensdiensten – eIDAS-Verordnung. Ein Überblick über die wichtigsten Inhalte und deren Konsequenzen für Unternehmen“, in: *Computer und Recht* 30(12), 825-832.

Spindler, Gerald und *Rockenbauch, Matti* (2013): „Die elektronische Identifizierung. Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste“, in: *Multimedia und Recht* 16(3), 139-148.

Stadler, Thomas (2011): „Verstoßen Facebook und Google Plus gegen deutsches Recht? - Ausschluss von Pseudonymen auf Social-Media-Plattformen“, in: *Zeitschrift für Datenschutz* 1(2), 51-58.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein und TU Dresden (2007): *Verkettung digitaler Identitäten – Untersuchung im Auftrag des Bundesministeriums für Bildung und Forschung*, https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

Wybitul, Tim und *Fladung, Armin* (2012): „EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs", in: *Betriebs-Berater (BB)* 67(8), 509-515.

The White House (2011): *National Strategy for trusted Identities in Cyberspace. Enhancing Online Choice, Efficiency, Security, and Privacy*, https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Technische Aspekte grenzüberschreitender Interoperabilität

Jens Bender

Im Juni 2012 hat die EU-Kommission einen Vorschlag für eine „Verordnung zu elektronischen Identitäten und Vertrauensdiensten für Transaktionen im elektronischen Binnenmarkt“ (kurz: *eIDAS-Verordnung*) vorgelegt.

In den folgenden zwei Jahren wurde dieser Vorschlag vom Europäischen Parlament und dem Rat der Europäischen Union, der Vertretung der Mitgliedstaaten, verhandelt. Die Verhandlungen zwischen diesen drei Organen, der *Trilog*, wurde im Februar 2014 abgeschlossen. Nach Verabschiedung im Rat und Parlament wurde die „Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ als Verordnung (EU) Nr. 910/2014 am 28. August 2014 im Amtsblatt bekanntgemacht[1] und trat 20 Tage später am 18. September 2014 in Kraft. Die einzelnen Regelungen entfalten gestaffelt Rechtswirkung, wesentliche Daten sind:

- ab 18. September 2015: freiwillige Anerkennung notifizierter Identitätssysteme
- ab 1. Juli 2016: die Regelungen zu den Vertrauensdiensten werden wirksam
- und schließlich ab 18. September 2018: verpflichtende Anerkennung notifizierter elektronischer Identitätssysteme.

Der Verordnungsvorschlag umfasst zwei Regelungsgebiete. Zum einen wird die europäische Signaturrichtlinie von 1999 abgelöst. Neben den bekannten elektronischen Signaturen werden auch elektronische Siegel („Signaturen für juristische Personen“), Zeitstempel, Zustelldienste[2] und Webseitenauthentisierung – zusammenfassend „Vertrauensdienste“ – europaweit reguliert. Durch den Wechsel vom Rechtsinstrument der Richtlinie zu dem einer Verordnung werden die enthaltenen Regelungen unmittelbar bindendes nationales Recht, d.h. es gibt keine nationale Umsetzungsgesetzgebung. Daher ist die Regelungstiefe tiefer als in der Signaturrichtli-

1 EU-ABl. L 257 v. 28.8.2014, 73.
2 Entsprechend in Deutschland De-Mail.

nie, auch wenn nicht die Detailliertheit der deutschen Signaturgesetzgebung erreicht wird. Zum anderen führt die Verordnung Regelungen zur gegenseitigen Anerkennung der elektronischen Identitätssysteme der Mitgliedsstaaten – in Deutschland die eID-Funktion des neuen Personalausweises – ein.

Für diesen Bereich der elektronischen Identitäten sieht die Verordnung den Mechanismus der *Notifizierung* vor, d.h. es wird keine „europäische elektronische Identität" entwickelt, sondern es soll ein technischer und organisatorischer Rahmen geschaffen werden, um existierende eID-Systeme der Mitgliedstaaten gegenseitig anzuerkennen. Dazu sollen – unter bestimmten Bedingungen – die Mitgliedstaaten einerseits ihre existierenden eID-Systeme *notifizieren*, andererseits für Anwendungen des öffentlichen Sektors alle notifizierten eID-Systeme verpflichtend *anerkennen*. Für eine rechtliche gegenseitige Anerkennung ist natürlich technische Interoperabilität notwendig.

Dieser Beitrag soll verschiedene technische Modelle zur Herstellung von (technischer) Interoperabilität von eID-Systemen beschreiben und deren Eigenschaften, sowohl aus Sicht der IT-Sicherheit als auch aus Sicht des Datenschutzes, bewerten.

1 Status Quo

Die grundsätzliche Idee, nicht eine einheitliche europäische elektronische Identität einzuführen, sondern auf die Interoperabilität bestehender Systeme hinzuarbeiten, ist aus der Tatsache begründet, dass in den letzten fünfzehn Jahren in vielen EU-Staaten nationale eID-Systeme eingeführt worden sind bzw. gerade eingeführt werden.

Als Beispiele seien hier als Repräsentanten einer großen Bandbreite von Verfahren der deutsche Personalausweis mit eID-Funktion, das niederländische DigID oder die österreichische Bürgerkarte genannt.[3] Bereits diese wenigen Beispiele zeigen, dass sich die Systeme in vielen wesentlichen Punkten unterscheiden:

3 Siehe http://www.personalausweisportal.de, https://www.digid.nl und http://www.buergerkarte.at. Vgl. auch ENISA 2009 für einen Überblick über verschiedene kartenbasierte europäische eID-Systeme.

- es gibt auf TANs basierende, Smartcard-basierte und Passwort-basierte Verfahren;
- es gibt Verfahren basierend ausschließlich auf eindeutigen Personenkennzeichen und Verfahren basierend auf einzelnen Identitätsattributen, ggf. sogar komplett ohne Personenkennzeichen;
- es gibt auf zentralen Infrastrukturen (Identity Provider) beruhende Verfahren und Verfahren, die ohne zentrale Komponenten arbeiten.

Schon anhand dieser wenigen Punkte wird klar, dass Interoperabilität nicht einfach herzustellen ist:

- die Verfahren bieten kein einheitliches Sicherheitsniveau;
- es gibt keinen gemeinsamen Satz von Identitätsattributen;
- in Systemen ohne zentrale Komponenten ist es schwierig, eine „zentrale Übersetzung" zwischen verschiedenen Verfahren vorzunehmen, ohne wesentliche Sicherheits- und/oder Datenschutzeigenschaften des Systems einzubüßen.

Die eIDAS-Verordnung schränkt diese Möglichkeiten nicht wesentlich ein. Grundsätzlich sollen nach Möglichkeit alle nationalen eID-Systeme notifizierungsfähig sein.

2 Was ist Identität?

Auf den ersten Blick scheint der Begriff der *Identität* einfach zu sein.[4] Die Identität einer Person ist eine Menge von Attributen, die die Person identifiziert. Mit dieser Definition wird das Problem aber nur sprachlich zur nächsten Ebene verschoben, da nun der Begriff *identifizieren* definiert werden muss.

Versucht man nun den Begriff *identifizieren* zu definieren, so kommt man nicht umhin, dem Verb auch eine handelnde Person zuzuordnen, d.h. es geht nicht darum, „mich" abstrakt zu identifizieren, sondern eine bestimmte andere (handelnde) Person will „mich" identifizieren. Daraus ergibt sich unmittelbar, dass *identifizieren* – und damit auch *Identität* – ein relativer, d.h. kontextbezogener, Begriff ist. Dies ist sowohl in der physischen als auch in der elektronischen Welt nichts Neues. Ich bin dem Staat gegenüber durch meine Identitätsdaten, wie sie in der Geburtsurkunde und

4 Für diesen Abschnitt vgl. auch [ISO/IEC 24760-1].

daraus folgend im Personalausweis, Reisepass usw. niedergelegt sind, bekannt. In anderen Bereichen bin ich nur durch einen Teil der Identitätsdaten bekannt – etwa nur durch den Vornamen im Freizeitbereich – oder auch durch ganz andere Daten, z.B. einen Spitznamen (Pseudonym). Wenn ich ein Kino besuche, interessiert sich der Betreiber nicht für meinen Namen, aber ggf. für das Identitätsattribut „volljährig".

Somit kann eine Person kontextbezogen viele verschiedene Identitäten haben. Auch die Erforderlichkeit der Eindeutigkeit der kontextuellen Identität ist anwendungsabhängig. In manchen Bereichen muss eine Identität eindeutig sein, in anderen nicht. Dabei ist auch noch zu unterscheiden, ob Eindeutigkeit in dem Sinne zu verstehen ist, dass eine Person genau eine Identität hat, oder aber in dem Sinne, dass niemand anderes die gleiche Identität hat. Erschwerend kommt hinzu, dass Identitätsattribute, die eine Person in einem Kontext eindeutig identifizieren können, dieses ggf. in einem anderen Kontext nicht tun. In der Familie ist eine Person oft bereits durch den Vornamen eindeutig identifiziert, am Arbeitsplatz meist nicht.

Verbindet man diese Überlegungen nun mit der datenschutzrechtlichen Notwendigkeit, grundsätzlich nur so wenige Daten (hier: Identitätsattribute) wie möglich zu verarbeiten, kommt man zu dem Ergebnis, dass auch ein elektronisches Identifizierungssystem nicht *die Identität* abbilden kann, sondern eher eine (anwendungsabhängige) Menge von Identitätsattributen zur Verfügung stellen muss, aus der dann erst der Empfänger der Attribute im Rahmen seiner Anwendung eine (anwendungsbezogene) Identität konstruiert.

Die Verordnung bleibt leider hinter diesem allgemeinen Begriff der Identität zurück. Der Begriff „Identifizierung" wird dort immer als „eindeutige Identifizierung" interpretiert. Dabei wird die Eindeutigkeit an der Gesamtheit der Bürger des notifizierenden Staates gemessen, d.h. es müssen hinreichend viele Identitätsattribute übermittelt werden, so dass etwa in einem Streitfall ein Bürger durch den notifizierenden Staat eindeutig ermittelt werden kann.

3 Begriffe

Neben den oben diskutierten Begriffen *Identität* und *Identitätsattribut* werden in diesem Artikel die folgenden Begriffe verwendet (vgl. auch die

technischen Standards in [ISO/IEC 24760-1] und [TR-03107-1] sowie die eIDAS-Verordnung):[5]

- Eine *Authentisierung* ist das Versehen einer Menge von Identitätsattributen (eine Identität) mit Metadaten, die es dem Empfänger ermöglichen, die Herkunft, Echtheit und Gültigkeit der Identitätsattribute zu überprüfen. Der Überprüfungsvorgang durch den Empfänger ist die *Authentifizierung* der Identität. Da beide Begriffe im englischen mit *authentication* übersetzt werden, werden sie auch im deutschen vermehrt gleichwertig genutzt, so auch zur Vereinfachung in diesem Artikel.
- *Authentisierungsmittel* sind technische Mittel, die es dem Inhaber erlauben, eine Identität (das heißt eine Menge von Identitätsattributen) zu authentisieren. Beispiele für Authentisierungsmittel sind Passwörter, der Personalausweis oder eine Signaturkarte.
- Ein *eID-System* (oder *Authentisierungssystem*) ist die Gesamtheit der technischen Infrastruktur einschließlich organisatorischer Prozesse und rechtlicher Rahmenbedingungen, die die Authentisierung und Authentifizierung mittels Authentisierungsmitteln ermöglichen.
- Zur Vereinfachung benutzt dieser Artikel verkürzend die Begriffe *Bürger* und *Dienstanbieter*[6] für den Sender und den Empfänger einer elektronischen Identität/Authentisierung.
- Eine *Identifizierung* ist die Übermittlung von anwendungsbezogen geeigneten Identitätsattributen (einer Identität), einschließlich authentisierender Metadaten (Authentisierung), sowie die Überprüfung (Authentifizierung) dieser Identität durch den Empfänger.

4 Anforderungen an ein eID-System

In diesem Abschnitt werden einige für die folgende Darstellung wichtige Eigenschaften von eID-Systemen vorgestellt. Ein Verbund von verschiedenen nationalen eID-Systemen kann als (sehr komplexes) eID-System

---

5 Die hier gegebenen Definitionen sind eingeschränkt auf den Anwendungsbereich der elektronischen Identifizierung. [ISO/IEC 24760-1] und [TR-03107-1] enthalten die Definitionen in allgemeinerer Form.

6 In der eIDAS-Verordnung werden die beiden Rollen mit *natural or legal person or natural person representing a legal person* bzw. *relying party* bezeichnet.

aufgefasst werden. Daher gelten diese Anforderungen auch für das angestrebte EU-weite Interoperabilitätsframework.

4.1 Datenminimierung

Ein eID-System kann eine feste Menge von Identitätsattributen anbieten, wenn es nur für eine Anwendung (bzw. mehrere Anwendungen mit gleichem Identitätsbegriff) eingesetzt wird. Ein wichtiges Beispiel für solche Anwendungen sind Anwendungen des eGovernment. In diesen wird immer eine Identifizierung anhand der staatlichen Identität notwendig sein. In vielen Ländern ist dies eine Personenkennziffer, in Deutschland oft die Kombination von Vornamen, Nachname/Geburtsname, Geburtsdatum und -ort.

Nun werden viele der existierenden nationalen eID-Systeme (so auch die eID-Funktion des deutschen Personalausweises) neben dem eGovernment auch für privatwirtschaftliche Anwendungen eingesetzt. Wie oben dargestellt, benötigen diese Anwendungen oft weniger oder andere Identitätsattribute. Der Einsatz des Interoperabilitätsmechanismus auch für privatwirtschaftliche Anwendungen wird in der eIDAS-Verordnung ausdrücklich vorgesehen.[7]

Aus diesen Gründen muss ein eID-System bzw. ein Interoperabilitätsmechanismus in der Lage sein, anwendungsbezogen unterschiedliche Mengen von Identitätsattributen zu übermitteln, um der datenschutzrechtlichen Anforderung der Datenminimierung nachzukommen. Es reicht nicht aus, dass erst die Anwendung die Daten auf das notwendige Maß reduziert bzw. nicht notwendige Attribute verwirft oder ignoriert. Dies wäre aus Sicht des Datenschutzes zu spät, weil die Daten unnötigerweise erhoben würden (*privacy by design*).

Auch wenn die Verordnung nur die eindeutige Identifizierung betrachtet (s.o.), ist es dennoch sinnvoll, auch in diesem Falle Mechanismen zur Datensparsamkeit vorzusehen. Dies ermöglicht die technische Nutzung des Interoperabilitätssystems auch für eine nicht-eindeutige Identifizierung, dies dann allerdings außerhalb des rechtlichen Rahmens der Verordnung.

---

7 Die eIDAS-Verordnung sieht eine verpflichtende Anerkennung nur für Dienstanbieter des öffentlichen Sektors vor, ermöglicht aber ausdrücklich eine freiwillige Anerkennung unter Nutzung des gleichen Interoperabilitätsframeworks für den privaten Sektor.

Darüber hinaus wird über eine attributsbasierte Identifizierung die Möglichkeit eröffnet, anwendungsbezogen notwendige weitere Attribute (z.B. die Wohnadresse) zu übermitteln.

4.2 Vertrauensniveau

Wie schon in der Einleitung gesehen, bilden die existierenden nationalen eID-Systeme die Identifizierung auf unterschiedlichen Sicherheitsniveaus ab. Für die Beurteilung eines Systems sind alle Komponenten mit ihren jeweiligen Sicherheitsanforderungen und -leistungen zu betrachten. Dies gilt neben der IT-Sicherheit auch für organisatorische Rahmenbedingungen, z.B. die Qualität des Enrolment in ein eID-System. Der Begriff *Vertrauensniveau* (*Assurance Level*) fasst die rein technische IT-Sicherheit mit diesen organisatorischen Anforderungen und der Vertrauenswürdigkeit der beteiligten Stellen zusammen.

Die eIDAS-Verordnung (Artikel 8 *Sicherheitsniveaus elektronischer Identifizierungssysteme*)[8] sieht die Bewertung der Zuverlässigkeit und Qualität[9] der folgenden Punkte vor:

- die Identitätsprüfung bei der Beantragung elektronischer Identifizierungsmittel;
- die Ausstellung des Identifizierungsmittels;
- der Authentifizierungsmechanismus selbst;
- die Einrichtung, die die Identifizierungsmittel ausstellt;
- jegliche andere Stelle, die im Antragsprozess involviert ist;
- die technischen Spezifikationen und die Sicherheitseigenschaften der Identifizierungsmittel.

Die verpflichtende Anerkennung ist eingeschränkt auf eID-Systeme, deren Vertrauensniveau hinreichend für die Anwendung ist (Artikel 6 *Gegenseitige Anerkennung*).

---

8 Der in der englischen Version verwendete Begriff des *Assurance Level* wird in der deutschen Fassung der Verordnung (etwas verkürzend) mit *Sicherheitsniveau* übersetzt, da das Wort *Vertrauen* bereits als Übersetzung von *confidence* im gleichen Artikel belegt ist. Dies ist leider nicht die einzige Stelle, in der die deutsche Übersetzung in Nuancen von der englischen Fassung abweicht.

9 In der englischen Fassung „reliability and quality".

Bestandteil der Sicherheitseigenschaften ist der Schutz der Integrität, der Authentizität sowie der Vertraulichkeit der Identitätsdaten. Hierfür ist relevant, an welchen Stellen die Identitätsdaten auf dem Weg vom Bürger zum Dienstanbieter verarbeitet werden. Sind die Daten auf dem Authentisierungsmittel des Bürgers selbst gespeichert und werden von dort Ende-zu-Ende verschlüsselt und integritätsgesichert übermittelt, so sind die Sicherheit und die Vertrauenswürdigkeit des Übermittlungsweges nicht relevant. Werden die Daten aber aus einem (zentralen) System abgerufen oder durch Systeme dritter Parteien verarbeitet (umgeschlüsselt bzw. neu integritätsgesichert), so sind Sicherheit und Vertrauenswürdigkeit dieser Systeme ebenso relevant.

Je höher das angestrebte Vertrauensniveau, desto wichtiger ist es, im Rahmen einer Authentisierung möglichst wenige Stellen an sicherheitsrelevanten Operationen zu beteiligen. Im Idealfall werden die Identitätsdaten Ende-zu-Ende verschlüsselt und integritätsgesichert übermittelt, d.h. es werden keine dritten Stellen beteiligt.

Vertrauensniveaus wurden bereits in vielen Projekten definiert. Durchgesetzt hat sich eine Einteilung in vier Niveaus bzw. Level. Einige Beispiele sind etwa.

- Hulsebosch et al. 2009: Im Rahmen des EU-Projekts STORK[10] wurde ein *Quality Authentication Assurance* framework (*QAA* framework) definiert.
- [ISO/IEC 29115]: Die ISO/IEC hat Kriterien für Vertrauensniveaus für die Identifizierung bzw. Authentisierung normiert.
- [TR-03107-1]: Für den Anwendungsbereich im deutschen eGovernment hat das BSI die Kriterien aus [ISO/IEC 29115] weiter detailliert und auf andere Anwendungsbereiche (Abgabe einer Willenserklärung, Dokumentenübermittlung) erweitert.

Die eIDAS-Verordnung sieht drei Vertrauensniveaus (*low*, *substantial* und *high*) vor, in etwa entsprechend den Leveln 2, 3 und 4 des STORK-Projekts (Hulsebosch et al. 2009) und [ISO/IEC 29115].

---

10 STORK ist die Abkürzung für *Secure idenTity acrOss boRders linKed*. Das Projekt wurde cofinanziert durch die EU-Kommission im Rahmen des *Competitiveness and Innovation Programme* und den Teilnehmern (16 von 27 Mitgliedstaaten, darunter auch Deutschland sowie die Nicht-EU-Mitglieder Norwegen und Island). Weitere Informationen unter https://www.eid-stork.eu. Zurzeit läuft das Nachfolgeprojekt STORK2, siehe https://www.eid-stork2.eu.

4.3 Gegenseitige Authentisierung

Voraussetzung für eine anwendungsbezogene Übermittlung von Identitätsattributen ist die Identifizierung der Anwendung bzw. des dazugehörigen Dienstanbieters vor Übermittlung der Attribute. Diese Identifizierung muss gegenüber dem Besitzer der Identitätsdaten – d.h. dem Bürger – erfolgen, da nur so dieser beurteilen kann, ob die Erhebung der Daten durch die Anwendung gerechtfertigt ist.

Auch [ISO/IEC 29115] verlangt eine gegenseitige Authentisierung („Mutual Authentication“) und die Verwendung einer kryptographischen Absicherung („Cryptographic Mutual Handshake“). Zwar ist dies keine feste Anforderung, sondern muss nur auf Basis einer Risikobewertung (*risk assessment*) umgesetzt werden. Aufgrund der Tatsache, dass „Mutual Authentication“ und „Cryptographic Mutual Handshake“ grundsätzlich als Anforderungen aufgezählt werden, kann man schließen, dass die Risikobewertung zumindest beim höchsten Vertrauensniveau (Level 4) zum Ergebnis kommen muss, dass diese Anforderungen umzusetzen sind.

Es reicht also nicht aus, dass sich lediglich der Bürger dem Dienstanbieter gegenüber identifiziert, sondern auch der Dienstanbieter muss sich (vorher) gegenüber dem Bürger auf dem entsprechenden Vertrauensniveau identifizieren.[11]

Diese notwendige gegenseitige Identifizierung als Bestandteil eines integrierten Gesamtprozesses ist ein wesentlicher Unterschied der elektronischen Identifizierung gegenüber dokumentenorientierten Verfahren wie z.B. fortgeschrittenen oder qualifizierten elektronischen Signaturen, bei denen nur der Signierende identifiziert wird, während die Signatur durch jeden verifizierbar ist, es also keinen vorab identifizierten Empfänger der Signatur gibt.[12]

Für ein Identifizierungsverfahren hingegen ist es vorteilhaft, wenn die übermittelten Identitätsdaten nur durch den identifizierten Empfänger,

---

11 Zumindest für das höchste Vertrauensniveau (Level 4) ist dabei SSL/TLS nicht ausreichend, wie die Vorfälle der letzten Jahre (Comodo, DigiNotar, usw.) zeigen.

12 Auch die eIDAS-Verordnung macht in der Definition für elektronische Signatur klar, dass sich eine Signatur immer auf bestimmte Daten (Dokumente) bezieht: „Elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden...“. Für die qualifizierte Signatur sieht die Verordnung eine rechtliche Wirkung (die Äquivalenz zur Unterschrift) vor, nicht jedoch für die Identifizierung (vgl. auch [TR-03107-1]).

nicht jedoch durch Dritte, verifizierbar sind. Dies entspricht auch der Situation in der physischen Welt, in der sich ein Bürger gegenüber einer bestimmten anderen Person (Behörde, Geschäftspartner, …) identifiziert, dieser Identifizierungsvorgang (z.B. durch Vorlage des Personalausweises) Dritten gegenüber aber nicht ohne weiteres nachweisbar ist.[13]

5 Grundsätzliche Ideen

In diesem Abschnitt werden verschiedene grundsätzliche Konzepte für ein Interoperabilitätsframework vorgestellt sowie deren jeweilige Vor- und Nachteile dargestellt.

5.1 Proxy/Gateway

Die Grundidee der Gateway-Lösung ist, nicht die eID-Systeme selbst interoperabel zu machen, sondern Interoperabilität mittels Übersetzungsgateways zu erzielen, die zwischen dem nationalen eID-System des Identitätsinhabers und dem System des Empfängers der Identitätsdaten vermitteln bzw. übersetzen.

In etwas erweiterter Form wurde dieses System im Rahmen des STORK-Projektes pilotiert. Hier wurde nicht ein Übersetzungsgateway eingesetzt, sondern ein Netzwerk von Gateways (*PEPS – Pan European Proxy Service*). Jeder Mitgliedstaat betreibt eines dieser Gateways (oder PEPS-Server). Möchte sich nun ein Bürger aus Mitgliedstaat A gegen einen Dienstanbieter aus Mitgliedstaat B authentisieren, so werden (etwas vereinfacht) folgende Schritte abgewickelt:[14]

1. Der Dienstanbieter stellt seine Identitätsanfrage an das Gateway seines Landes (PEPS-B); diese Anfrage enthält seine eigene Identität und das angeforderte Vertrauensniveau. Diese Anfragedaten reicht PEPS-B an den Bürger weiter.

---

13 Selbst wenn der Empfänger der Identifizierung eine Ausweiskopie anfertigt, hat diese gegenüber dem Ausweis selbst einen wesentlich geringeren Wert als Identifizierungsmittel.

14 Vgl. Berbecaru et al. 2011: 38.

2. Der Bürger teilt PEPS-B mit, welcher PEPS für ihn zuständig ist, woraufhin PEPS-B die Anfragedaten an den so ausgewählten PEPS-A weiterreicht.
3. Der Bürger authentisiert sich mit seinem nationalen eID-System gegenüber dem Gateway-Server seines Landes (PEPS-A). Diese Kommunikation ist landesspezifisch entsprechend dem nationalen eID-System, und involviert ggfs. einen Identitätsprovider (IdP).

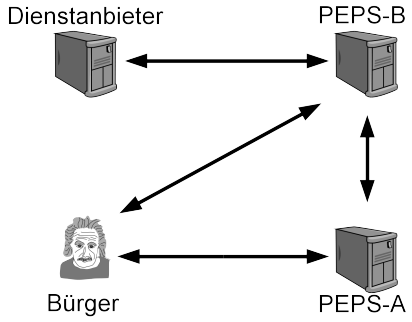

Abbildung 1: Kommunikation Gateway

4. Die authentisierte Identität wird von PEPS-A an den Gateway-Server des Landes des Dienstanbieters (PEPS-B) weitergegeben. Diese Kommunikation erfolgt nach einem im STORK-Projekt standardisierten Verfahren, das auf SAML (Security Assertion Markup Language) basiert.
5. PEPS-B gibt die authentisierte Identität an den Dienstanbieter weiter, wiederum gemäß der STORK-Spezifikationen.[15]

Prinzipbedingt gibt es bei diesem Verfahren keine Ende-zu-Ende-Sicherheit. Sowohl PEPS-A als auch PEPS-B entschlüsseln die Identitätsdaten und verschlüsseln sie neu, ebenso werden die Daten neu durch die Gateways authentisiert. Damit ist aber auch keine gegenseitige Authentisierung auf hohem Sicherheitsniveau möglich.

---

15 Die Kommunikation zwischen PEPS-A und PEPS-B einerseits und PEPS-B und Dienstanbieter andererseits erfolgt *nutzer-zentriert* („*user centric*"), d.h. die Kommunikation erfolgt nicht direkt, sondern mittels Weiterleitung (und Zustimmung) über den Browser des Bürgers. Um die Zustimmung des Bürgers zu ermöglichen, werden die Identitätsdaten auf diesen Strecken lediglich auf Transportebene verschlüsselt (TLS/SSL).

Da die Identitätsdaten bei den Gateways im Klartext vorliegen, ist es unerlässlich, dass jeder Nutzer (sowohl Bürger als auch Dienstanbieter) sowohl dem Gateway seines Landes als auch dem Gateway des anderen beteiligten Landes vertrauen kann. Wichtig ist dabei festzuhalten, dass es nicht ausreicht, dass das Gateway bzw. dessen Betreiber tatsächlich *vertrauenswürdig* ist, sondern dass zusätzlich der Bürger auch dem Betreiber *vertrauen* muss, d.h. die behauptete Vertrauenswürdigkeit glauben muss – schon der Verdacht der fehlenden Vertrauenswürdigkeit kann zu einem Vertrauensverlust beim Bürger und damit der Ablehnung des gesamten Systems führen.

Die Frage, ob Bürger einem (staatlich betriebenen) zentralen Gateway hinreichend vertrauen, kann hier natürlich nicht abschließend beantwortet werden.

Aus technischer und organisatorischer Sicht stellt sich die Gateway-Lösung hingegen aus mehreren Gründen als problematisch dar, die sich negativ sowohl auf die Vertrauenswürdigkeit als auch auf das entgegengebrachte Vertrauen auswirken können.

Das Gateway besitzt prinzipbedingt viele Informationen, insbesondere Informationen darüber, welcher Bürger sich wann und wo authentisiert. In eID-Systemen, die von vornherein auf eine zentrale Authentisierungskomponente aufbauen, ist dies kein (neues) Problem. Dagegen wird für eID-Systeme, die bewusst auf einen dezentralen Aufbau setzen (wie der deutsche Personalausweis), dieses Prinzip durchbrochen.

Dabei ist zu beachten, dass ein dezentraler Aufbau nicht nur aus Gründen des Datenschutzes vorteilhaft sein kann, sondern auch aus dem Blickwinkel der Verfügbarkeit des eID-Systems. Bei einem dezentralen System führt der Ausfall einer Komponente nur zu einer lokalen Nicht-Verfügbarkeit, während der Ausfall einer zentralen Komponente sofort zu einem Komplettausfall führt. Sowohl aus Sicht der verfügbaren Daten als auch aus Sicht der öffentlichen Wirkung eines erfolgreichen Angriffs ist eine zentrale Komponente auch immer ein bevorzugtes Ziel für Angreifer.

Der wesentliche Vorteil der Gateway-Lösung ist die einfache Integration für Dienstanbieter. Diese müssen lediglich einmal die Schnittstelle zu dem Gateway ihres Landes implementieren und können dann weitgehend automatisch alle eID-Systeme verwenden.

Insbesondere der letzte Aspekt hat die EU-Kommission dazu veranlasst, ihren Verordnungsvorschlag – zumindest implizit – auf diesem Modell aufzubauen.

5.2 Middleware

Eine Alternative zur Gateway-Lösung ist ein Interoperabilitätsframework basierend auf einer gemeinsamen Middleware. Bei diesem Ansatz erfolgt die Übersetzung zwischen verschiedenen eID-Systemen nicht durch zentrale Gateways, sondern durch eine (dezentral) beim Dienstanbieter installierte Middleware. Der Ablauf einer Authentisierung ist dann wie folgt:

1. Zunächst wählt der Bürger auf der Webseite des Dienstanbieters sein eID-System aus.
2. Daraufhin übersendet der Dienstanbieter eine Identitätsanfrage an den Bürger. Diese Anfrage enthält die (authentisierte) Identität des Dienstanbieters sowie ggf. eine Liste angefragter Identitätsattribute. Diese Daten werden durch die Middleware-Komponente entsprechend der Vorgaben des eID-Systems des Bürgers übersandt.
3. Der Bürger übersendet nach entsprechender Freigabe die angefragten Identitätsattribute an den Dienstanbieter (repräsentiert durch die dort implementierte Middleware-Komponente), wo diese geprüft und verarbeitet werden.

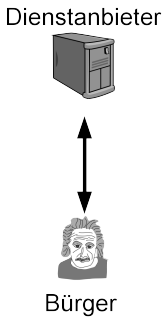

Abbildung 2: Kommunikation Middleware

Bei entsprechender kryptographischer Ausgestaltung des eID-Systems erfolgt sowohl die Identifizierung des Dienstanbieters als auch die Übersendung der Identitätsattribute durch den Bürger in einem Ende-zu-Ende-Kanal zwischen diesen beiden Kommunikationspartnern.

Ein wesentlicher Unterschied zur Gateway-Lösung ist damit, dass die Übersetzungsleistung nicht durch einen (datenschutzrechtlich unabhängigen) Dritten erfolgt, sondern unmittelbar in der datenschutzrechtlichen

Verantwortung des Dienstanbieters. Dies entspricht der deutschen Rechtslage in Bezug auf den Personalausweis. Die dienstanbieterseitige Middleware-Komponente ist definiert als *eID-Server* in [TR-03130].

Gerade diese unmittelbare Verantwortung des Dienstanbieters hat aus Sicht des Bürgers deutliche Vorteile. Bei einem Gateway-basierten System ist im Falle einer fehlgeschlagenen Authentisierung oder bei Kompromittierung und Missbrauch der Identitätsdaten für den Bürger a priori nicht klar, ob der Fehler beim Dienstanbieter oder bei einem der beteiligten Gateways liegt. Damit ist aus Bürgersicht auch nicht unmittelbar erkennbar, an wen er sich z.B. bezüglich einer etwaigen Haftung zu wenden hat oder welches die zuständige Datenschutz-Aufsichtsbehörde ist. Im schlimmsten Fall sind sich auch der Dienstanbieter und die Gateway-Betreiber nicht einig, wer die Haftung trägt, mit entsprechenden Schwierigkeiten für den Bürger.

Zwar sieht die eIDAS-Verordnung eine Haftung der Mitgliedstaaten für ihre eID-Systeme einschließlich der ggf. genutzten Gateways vor, allerdings ist dazu zunächst die Zuordnung des Fehlers zu einem eID-System oder einem der beteiligten Gateways notwendig. Zumindest der Dienstanbieter und das Gateway des eigenen Mitgliedstaates des Bürgers sind in unterschiedlichen Rechtsräumen angesiedelt und unterliegen damit unterschiedlichen Haftungsregimes. Im Ergebnis gibt es für den Bürger keinen einheitlichen Ansprechpartner bei Problemen.

Anders sieht dies im Falle der Middleware aus. Die Interoperabilitätskomponente ist unmittelbar dem Dienstanbieter zuzuordnen, unabhängig davon, ob er diese tatsächlich selbst betreibt oder sie über vertragliche Auftragsdatenverarbeitung an einen externen Dienstleister auslagert.[16] Aus Sicht des Bürgers ist immer der Dienstanbieter der alleinige Ansprechpartner bei Problemen mit den übertragenen Identitätsdaten.

Nicht nur aus rechtlicher, sondern auch aus technischer Sicht reduziert der Middleware-Ansatz deutlich die Komplexität der Kommunikationsszenarien, da lediglich der Bürger und der Dienstanbieter ohne Beteiligung Dritter miteinander kommunizieren (sofern das eID-System selbst

16 Es ist zu erwarten, dass zumindest in der Aufbauphase die meisten Dienstanbieter einen Auftragsdatenverarbeiter beauftragen, um den Integrationsprozess zu vereinfachen. Dadurch ist der Aufwand für den Dienstanbieter nicht wesentlich unterschiedlich von der Gateway-Lösung. Wesentlich ist die rechtliche Zuordnung des Auftragsdatenverarbeiters zum Dienstanbieter und damit eine einheitliche datenschutzrechtliche Verantwortlichkeit.

nicht bereits dritte Stellen, etwa einen Identity Provider, involviert). Andererseits erhöht dieses Szenario die Komplexität für den Dienstanbieter, da dieser (über die Middleware) mit jedem eID-System direkt kommunizieren muss.

Diese Komplexität kann jedoch durch geeignete Spezifikationen und Anforderungen an die Notifizierung von eID-Systemen reduziert werden. Wesentlich ist eine klare Schnittstellenspezifikation zur Integration neuer eID-Systeme. Ist diese Schnittstelle hinreichend präzise und geeignet, alle Varianten an eID-Systemen abzudecken, können neue Systeme über *Plug-Ins* integriert werden, d.h. ohne die Middleware selbst anpassen zu müssen. Über die Anforderungen an die Notifizierung von eID-Systemen können notifizierende Mitgliedstaaten dazu verpflichtet werden, für ihr eID-System ein Plug-In frei zur Verfügung zu stellen und zu pflegen.

Um die Verteilung zu vereinfachen, können sowohl die eigentliche Middleware selbst als auch die Plug-Ins über einen zentralen Service zur Verfügung gestellt werden. Über diesen Service könnten sich Dienstanbieter regelmäßig sowohl mit der aktuellen Middleware als auch mit einem aktuellen Satz an Plug-Ins versorgen.

Grundsätzlich kann bei diesem dezentralen System jeder Dienstanbieter selbst bestimmen, mit welchen Verfügbarkeitsanforderungen er sein System betreiben will und entsprechend Aufwand und Verfügbarkeitsanforderungen gegeneinander ausbalancieren. In einem zentralen Gateway-basierten System muss sich das Gateway nach den höchsten Verfügbarkeitsanforderungen aller angeschlossenen Dienstanbieter richten, also im allgemeinen Hochverfügbarkeit zusichern – mit den entsprechenden Aufwänden für den Betreiber, die dieser voraussichtlich auf die Dienstanbieter umlegt bzw. die durch den Staat übernommen werden müssen.

Natürlich kann in einem Middleware-basierten Interoperabilitätsframework auch ein PEPS-Netzwerk integriert werden. Dieses Netzwerk erscheint dann aus Sicht der Middleware als (eines von mehreren) eID-Systemen. Diese Kombination (einschließlich des Plug-In-basierten Ansatzes) wurde in STORK unter dem Begriff *Virtual Identity Provider* (VIdP) pilotiert.[17] Sie ermöglicht es, für hohes Vertrauensniveau eine Ende-zu-Ende-Verbindung zu nutzen (dann über eine direkte Kommunikation des Bürger-eID-Systems mit der Middleware), im Falle eines niedrigeren Vertrau-

17 Sowohl die PEPS-Software als auch die VIdP-Software stehen unter https://joinup.ec.europa.eu/software/stork/release/all zur Verfügung.

ensniveaus aber auf das ggf. einfacher zu integrierende PEPS-System auszuweichen.

5.3 Gemeinsame Spezifikation

Einen Schritt weiter als die Middleware-Lösung geht der Ansatz, die verschiedenen eID-Systeme direkt interoperabel zu gestalten. Da dies eine Veränderung der nationalen Systeme bedeutet, geht dies über den in der eIDAS-Verordnung vorgesehenen Ansatz der reinen Notifizierung hinaus. In vielen (nicht allen) Mitgliedstaaten basieren die eID-Systeme auf nationalen Identitätskarten (in Deutschland der Personalausweis), die gleichzeitig hoheitliche nationale Dokumente sind. Daher kann eine Konvergenz zu einer gemeinsamen Spezifikation nur als freiwillige Zusammenarbeit von Mitgliedstaaten gestaltet werden.[18]

Grenzüberschreitende Interoperabilität setzt nicht voraus, dass die eID-Systeme identisch sind. Voraussetzung ist lediglich die Nutzung gemeinsam spezifizierter Datenformate und PKI-Strukturen. Eine Möglichkeit ist die gemeinsam von den französischen und deutschen IT-Sicherheitsbehörden ANSSI (*Agence nationale de la sécurité des systèmes d'information*) und BSI (*Bundesamt für Sicherheit in der Informationstechnik*) mit Unterstützung der französischen und deutschen Smartcard-Industrie vorangetriebene *eIDAS-Token-Spezifikation*.[19] Dies ist eine gemeinsame Spezifikation für Smartcard-basierte elektronische Identitäten. Technologisch basiert die Spezifikation auf der (auch im deutschen Personalausweis) eingesetzten *Extended Access Control*-Technologie, die bereits europaweit für die Sicherung der Fingerabdrücke im elektronischen Reisepass eingesetzt wird.[20]

---

18 Nach Artikel 77 Abs. 3 AEUV kann der Rat per einstimmigen Beschluss Regelungen zu Personalausweisen erlassen, allerdings nur zur Erleichterung der Umsetzung der Freizügigkeit der Unionsbürger, d.h. für den physischen Grenzübertritt.

19 Siehe https://www.bsi.bund.de/eIDAS.

20 Siehe z.B. Kügler und Naumann 2007.

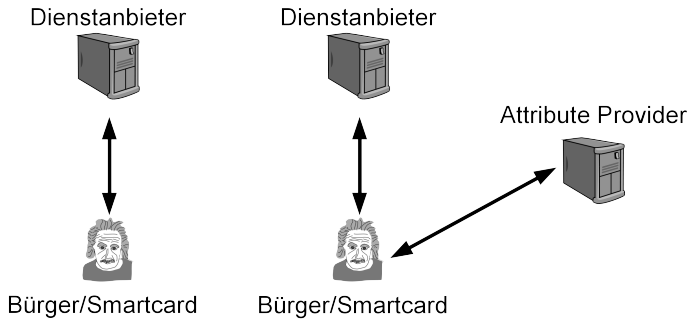

Abbildung 3: eIDAS-Token: System ohne und mit Attribute Provider

Die Spezifikation erlaubt sowohl eID-Systeme ohne Identity Provider (wie den deutschen Personalausweis) als auch eID-Systeme mit *Attribute Providern*. Wesentlicher Unterschied zwischen einem System mit Attribute Provider im Sinne dieser Spezifikation und einem mit einem klassischen Identity Provider ist dabei, dass nicht der Dienstanbieter mit dem Identity Provider kommuniziert, sondern der Bürger bzw. die Smartcard mit dem Attribute Provider. Dadurch entfällt – bei entsprechender Ausgestaltung – das grundsätzliche Problem von eID-Systemen mit Identity Providern, dass diese vollständige Informationen über alle Authentisierungsvorgänge haben. Weiterhin ist die Dienstanbietersicht auf das System in beiden Ausgestaltungen identisch: Dieser kommuniziert ausschließlich mit dem Bürger bzw. dessen Smartcard, entsprechend einer einheitlichen Schnittstellenspezifikation.

Eine gemeinsame technische Basis der eID-Systeme kann langfristig zu einer Vereinfachung des Interoperabilitätsproblems führen, vermag aber kurzfristig nicht ein Interoperabilitätsframework auf Basis von Gateways oder Middleware zu ersetzen.

6 Zertifikate

Unabhängig vom gewählten Interoperabilitätsframework müssen als Teil des Aufbaus und Betriebs Zertifikate ausgetauscht werden. Jeder Dienstanbieter muss in der Lage sein, die Echtheit und Gültigkeit der erhaltenen Identitätsdaten zu prüfen (authentifizieren). Im Allgemeinen benutzen eID-Systeme dazu eine PKI, deren Wurzelzertifikate allen Dienstanbietern

bekannt sein müssen. Die Verteilung der Zertifikate muss dabei auf vertrauenswürdigem Wege erfolgen.

Wird ein Gateway-basiertes Interoperabilitätsframework genutzt, so genügt es, wenn die Zertifikate an den Gateways bekannt sind. Zur Überprüfung der Nachrichten der Gateways müssen aber bei den Dienstanbietern zumindest die Zertifikate der Gateways selbst bekannt sein und diesen durch die Dienstanbieter vertraut werden.

Im Falle eines Middleware-basierten Frameworks müssen die Zertifikate direkt beim Dienstanbieter bekannt sein. Eine Verteilung kann z.B. als Bestandteil des Verteilmechanismus für aktualisierte Plug-Ins erfolgen, sofern dieser geeignet abgesichert ist. Auf diese Weise ist der Aufwand für den Dienstanbieter nicht höher als im Gateway-basierten Fall, er muss lediglich das Zertifikat zur Verifikation der Plug-Ins kennen und diesem vertrauen.

Ein vertrauenswürdiger Verteilmechanismus für weitergehende Statusinformation ist ebenfalls notwendig (und kann auf dem gleichen Prinzip beruhen), da die eIDAS-Verordnung auch die (ggf. temporäre) Suspendierung von eID-Systemen (oder Teilen davon, etwa einer bestimmten Generation von ID-Karten), etwa im Falle der Kompromittierung des (Teil-)Systems, vorsieht.[21]

Etwas aufwendiger ist der Fall der Zertifikatsverteilung für eID-Systeme, in denen eine explizite PKI-basierte Identifizierung der Dienstanbieter erforderlich ist. Ein Beispiel für ein solches System ist das System der *Berechtigungszertifikate* beim deutschen Personalausweis. Jeder Dienstanbieter erhält ein Zertifikat, das im Zuge der gegenseitigen Authentisierung durch den Ausweischip verifiziert wird. Dieses Zertifikat enthält sowohl Angaben zur Identität des Dienstanbieters (und ermöglicht damit die gegenseitige Authentisierung) als auch Angaben zu den Identitätsattributen, die der Dienstanbieter abfragen darf (und ermöglicht damit die technische Durchsetzung des Prinzips der Datenminimierung).

Dazu wird in der Produktion das Zertifikat der Wurzelinstanz (Root) der zugehörigen PKI auf dem Chip gespeichert. Die Wurzelinstanz zertifiziert SubCAs (in Deutschland: Berechtigungs-CAs), die wiederum die Zertifikate für die Dienstanbieter als Endnutzerzertifikate ausstellen.

---

21 Vgl. eIDAS-Verordnung, Artikel 10 *Sicherheitsverletzung*.

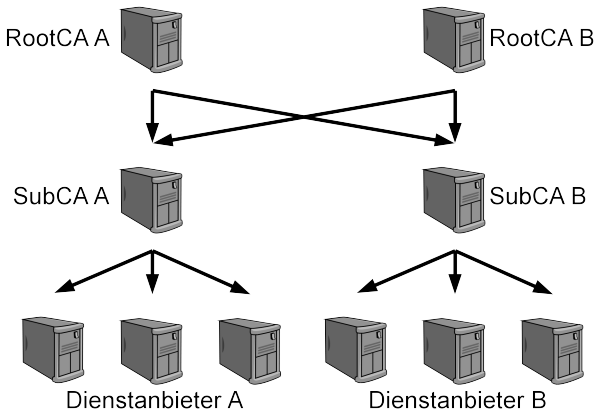

Abbildung 4: Cross-Zertifizierung

Mehrere eID-Systeme mit Berechtigungszertifikaten können durch *Cross-Zertifizierung* interoperabel werden. Voraussetzung dafür ist die Nutzung kompatibler Zertifikatsformate in den verschiedenen eID-Systemen. Unter dieser Bedingung können nun die SubCAs zusätzlich zur Zertifizierung in ihrem „Heimatsystem" auch in den PKIen anderer eID-Systeme registriert bzw. zertifiziert werden. Dann muss nicht jeder Dienstanbieter ein Berechtigungszertifikat in allen eID-Systemen beantragen, sondern es reicht die Registrierung in einem System. Über die Cross-Zertifizierung gibt es gültige Zertifikatsketten von allen Wurzelinstanzen aus bis zu den einzelnen Dienstanbietern.

Ein entsprechendes System der Cross-Zertifizierung wird auch beim europäischen elektronischen Reisepass eingesetzt. Jeder Mitgliedstaat betreibt eine PKI für den Zugriffsschutz für die im Chip gespeicherten Fingerabdruckdaten. Die nationalen Wurzelinstanzen stellen Cross-Zertifikate für andere Mitgliedstaaten aus, um auf diesem Wege den Kontrollbehörden der anderen Mitgliedstaaten kontrollierten Zugriff auf die Fingerabdruckdaten zu gewähren. Dieses System umfasst auch die Spezifikation für automatisierte Kommunikationsprotokolle für den Zertifikatsaustausch, welche sich für den Fall der Zertifikatsverteilung für die Zertifizierung der Dienstanbieter weiterverwenden lassen.

7 Interoperabilitätsframework

Die folgende Tabelle fasst die gemachten Beobachtungen gegenüberstellend zusammen. Dabei werden nicht die Eigenschaften der zugrunde liegenden einzelnen eID-Systeme betrachtet, sondern nur die durch die jeweiligen Interoperabilitätsframeworks hinzukommenden.

	Gateway	**Middleware**	**Gemeinsame Spezifikation**
Direkte Ende-zu-Ende-Beziehung	Nicht möglich	Möglich, wenn Middleware Teil des Dienstanbieters	Möglich / Systemabhängig
IT-Sicherheit / zusätzliche Angriffsmöglichkeiten	Gateway ist zentraler Angriffspunkt	Keine neue Rolle, Eigenschaften der eID-Systeme bleiben erhalten	N/A
Datenschutz und Datenminimierung	Zentrales Tracking möglich; Umschlüsselung notwendig	Keine neue Rolle, Eigenschaften der eID-Systeme bleiben erhalten	Direkte Ende-zu-Ende-Beziehung und Berechtigungszertifikat möglich
Zusätzliche Komplexität des Systems	Hoch	Mittel	Keine
Zusätzliche Komplexität für den Dienstanbieter	Niedrig	Hoch; Wesentlich reduzierbar durch Plug-In-Lösung	Keine (ohne Berechtigungszertifikate); Mittel (mit Berechtigungszertifikaten)
Zusätzliche Komplexität für den Bürger	Mittel	Niedrig	Keine

Unabhängig davon, auf welcher Basis ein Interoperabilitätsframework im Rahmen der eIDAS-Verordnung geschaffen wird, muss dieses (mindestens) die folgenden Punkte umfassen:

- Definition geeigneter Vertrauensniveaus. Dabei müssen die Definitionen einerseits umfassend und präzise genug sein, um eID-Systeme objektiv bewerten zu können, andererseits dürfen keine bestimmten Technologien a priori ausgeschlossen werden.
- Definition von Identitätsattributen und Austauschformaten. Interoperabilität von eID-Systemen setzt auch voraus, dass die in einem System verfügbaren Daten von den anderen Systemen verstanden werden. Dies startet bei der grundsätzlichen Festlegung eines minimalen verfügbaren

Datensatzes (z.B. für Deutschland relevant: gibt es die Anforderung der Verfügbarkeit eines eindeutigen Merkmals?),[22] umfasst die einheitliche Definition von Datenfeldern (sind Vorname/Nachname ein oder zwei Datenfelder? Was geschieht bei Ländern mit anderem Namenskonzept – z.B. Patronym statt Familiennamen?), und schließlich auch die Kodierung der einzelnen Datenfelder (wie wird mit Daten in nichtlateinischen Alphabeten umgegangen, etwa griechisch oder kyrillisch?).

- Spezifikation der Interoperabilitätskomponenten. Unabhängig vom gewählten Ansatz (oder der Kombination mehrerer Ansätze) müssen die Schnittstellen hinreichend präzise spezifiziert werden.
- Konformitätsprüfungen. Um Interoperabilität dauerhaft sicherzustellen, ist es notwendig, die verschiedenen teilnehmenden Komponenten auf Konformität zu den Spezifikationen zu prüfen. Ein reiner Cross-Over-Test, d.h. ein Test gegen andere Implementierungen, reicht erfahrungsgemäß nicht aus, da dann jegliche – spezifikationskonforme – Implementierungsänderung bei anderen Komponenten zu Problemen führen kann.
- Austausch von Zertifikaten und Statusinformationen. Sowohl für die Prüfung der Echtheit elektronischer Identitätsdaten als auch ggf. für die Zugriffskontrolle ist der vertrauenswürdige Austausch von Zertifikaten notwendig. Insbesondere der Austausch von Wurzelzertifikaten muss auf sicherem Wege erfolgen, da diese die Vertrauensanker für das gesamte System bilden. Für die Verteilung von Berechtigungszertifikaten ist ein automatisierter Mechanismus notwendig.

Es ist sicherlich sinnvoll, hier auf die Erfahrungen aus anderen europäischen Interoperabilitätsprojekten zurückzugreifen, beispielsweise die Einführung interoperabler elektronischer Reisepässe, bei deren Spezifikation und Einführung ähnliche Probleme zu lösen waren.

---

22 In Deutschland gibt es kein eindeutiges Personenmerkmal („Personenkennziffer"). Dies betrifft auch andere Länder, in denen z.B. eine existierende Personenkennnummer ausschließlich für die nationale Verwaltung, also nicht grenzüberschreitende, verwendet werden darf.

8 Aktueller Stand

Die hier besprochenen Aspekte der Interoperabilität – insbesondere Vertrauensniveaus und technische Interoperabilität – werden über Durchführungsrechtsakte reguliert, die rechtzeitig zum Beginn der freiwilligen gegenseitigen Anerkennung, dem 18. September 2015, verabschiedet wurden.

Für die technische Interoperabilität sieht der entsprechende Durchführungsrechtsakt sowohl die Möglichkeit der gateway-basierten als auch der middleware-basierten Notifizierung vor, d.h. der notifizierende Mitgliedstaat legt fest, welche der beiden Varianten für die Interaktion mit „seinem" eID-System genutzt wird. Dies entspricht der Situation im STORK-Projekt, in dem beide Varianten pilotiert wurden. Jedoch gibt es einige Fortentwicklungen gegenüber diesem Projekt, z.B. die Anpassung des Datenmodells an die Anforderungen der eIDAS-Verordnung, die Ergänzung der Verschlüsselung von Identitätsattributen und Festlegungen zum Schlüsselmanagement. Die technischen Details werden nicht im Durchführungsrechtsakt selbst geregelt, sondern durch nachgelagerte technische Spezifikationen, die in Kooperation von den Mitgliedstaaten festgelegt werden.[23]

Ab dem Zeitpunkt der Verabschiedung der Durchführungsrechtsakte bleiben den Mitgliedstaaten noch drei Jahre bis zur verpflichtenden Anerkennung aller notifizierten eID-Systeme, d.h. in dieser Zeit müssen die Spezifikationen von allen Dienstanbietern des öffentlichen Sektors umgesetzt werden. In Anbetracht der Komplexität der Aufgabe ist dies ein ausgesprochen knapper Zeitplan, da Anpassungen bei jedem Dienstanbieter des öffentlichen Sektors notwendig sind.

Im Ergebnis ist die Verordnung – und auch die Durchführungsrechtsakte – ein typisch europäischer Kompromiss, wie exemplarisch an der Festlegung sichtbar wird, sowohl gateway- als auch middleware-basierte Notifizierungen zuzulassen. In Anbetracht des Zeitdrucks scheint dies der einzig gangbare Weg zu sein. Langfristig ist jedoch eine Fortentwicklung des Systems erforderlich, um Anforderungen der IT-Sicherheit und des Datenschutzes von vornherein im System zu verankern. Ein gemeinsames Verständnis und die Definition geeigneter Migrationsszenarien vorausgesetzt,

23 Version 1.0 der Spezifikationen ist veröffentlicht unter https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v 10.

scheint die Konvergenz zu einer gemeinsamen (europäischen) Konzeption und Spezifikation sinnvoll zu sein.

Literatur

Berbecaru Diana, Jorquera Eva, Schiavo Martine, Johnston Adrian, Lioy Antonio, Axfjörð Arnaldur F., Luyten Carlo, Ribeiro Carlos, Orthacker Clemens, Martínez Daniel, Alcalde-Moraño Joaquín, Felix Luís, Stern Marc, Stoltz Mario, Schwan Matthias, Portela Renato, Másson Sigurður, Martens Tarvi, Rössler Thomas and *Bauer Wolfgang* (2011): *STORK-Projekt: Deliverable D5.7.3 „Functional Design for PEPS, MW models and interoperability (v 3)"*, https://www.eid-stork.eu.

European Network and *Information Security Agency (ENISA)* (2009): *Position Paper „Privacy Features of European eID Card Specifications"*, http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-cards-en.

Hulsebosch Bob, Lenzini Gabriele and *Henk Eertink* (2009): *STORK-Projekt: Deliverable D2.3 „Quality authenticator scheme"*, https://www.eid-stork.eu.

Kügler, Dennis und *Naumann, Ingo* (2007): „Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass", in: *Datenschutz und Datensicherheit* 31 (3), 176-180.

Technische Standards:

[ISO/IEC 24760-1] ISO/IEC 24760-1: Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts, 2012.

[ISO/IEC 29115] ISO/IEC 29115: Information technology — Security techniques — Entity authentication assurance framework, 2013.

[TR-03107-1] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03107-1: Elektronische Identitäten und Vertrauensdienste im eGovernment — Teil 1: Vertrauensniveaus und Mechanismen, 2014.

[TR-03130] Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-03130: eID-Server, 2014.

Where is the knowledge we have lost in information?[1] Die soziale Dimension von Privatheit und Identität in Indien

Tile von Damm

1 Identitätsmanagement als globales Problem

Identitätsmanagement ist ein nicht nur in westlichen Staaten, sondern weltweit diskutiertes Problem. Die sichere (digitale) Organisation zur eindeutigen Erkennung und Wiedererkennung der Mitglieder des Gemeinwesens ist auch in Indien eine zentrale Herausforderung, da die eindeutige Identifizierung einerseits Grundlage zahlreicher staatlicher Programme ist, andererseits Zugang zum Gemeinwesen verspricht. Bei allen grundsätzlichen Parallelen mit anderen Staaten zeigen sich jedoch soziokulturell, rechtlich und politisch unterschiedliche Voraussetzungen und Rahmenbedingungen, die in diesem Kapitel exemplarisch für Indien diskutiert werden.

Indien ist dabei aus mehreren Gründen ein überaus spannender Untersuchungsgegenstand. Die größte Demokratie der Welt weist eine hoch fragmentierte Gesellschaft auf, die sich durch ihre Heterogenität soziokulturell wesentlich von westlichen Staaten unterscheidet. Im Jahre 2015 lebten offiziell 1,293 Milliarden Einwohner in Indien,[2] von denen nach Schätzungen rund ein Viertel keine Ausweispapiere besitzt, um sich eindeutig identifizieren zu können. Die Gründe dafür sind vielfältig und spiegeln zunächst vor allem die faktische Lebensrealität des Einzelnen wieder, in der nicht nur Identitätspapiere kaum eine Rolle spielen, sondern die Interaktion zwischen Behörde und Bürger auch oftmals negative Konsequenzen nach sich zieht. Das indische Governancesystem weist eine hohe Ineffizienz auf, die durch koloniale Strukturen und Korruption geprägt ist. Die Fragen der Inklusion stellen sich in Indien also vollkommen anders als in homogenen Gesellschaften und müssen inhärent mitberücksichtigt werden, wenn IT-Infrastrukturen implementiert werden. Die Einführung von

1 Eliot 1934.
2 S. http://www.indiaonlinepages.com/population/india-current-population.html.

Identitätsmanagementsystemen umfasst deshalb grundlegende Fragen der zukünftigen Organisation des indischen Gemeinwesens. Auch wenn eine breite Diskussion in Indien zu diesen spezifischen Fragen nicht stattfindet, zeigt sich jedoch eine demokratische Auseinandersetzung über die ihnen zugrundeliegenden Probleme. Diese umfasst vor allem die Fragen nach Inklusion, Datensicherheit und Datenschutzschutz, technischer Unabhängigkeit von ausländischen Staaten und Konzernen und letztlich nach der rechtlichen Gestaltung in Anlehnung und Auseinandersetzung mit internationalen Vorbildern.

2 Rahmenbedingungen

Das Ringen um Identitätsmanagement, Datenschutz und Privatheit sowie offene Technologiestandards ist in Indien weit mehr als nur eine „sophisticated" Debatte. Vielmehr sind ihre konsequente Einführung und Ermöglichung zuvorderst soziale Fragen und entscheiden somit über den Zugang zur Gesellschaft als gleichberechtigtes Individuum. Dass die Feststellung der Identität des Einzelnen im Sinne einer Personenstandsfeststellung den Zugang zum indischen Gemeinwesen erst ermöglicht, ist ein wesentlicher Fakt im Hinblick auf die Funktionsfähigkeit einer demokratischen Gesellschaft. Die zahlreichen Versuche einer zentralen elektronischen Feststellung der Identität zeigen jedoch, dass es enorme Defizite des Governancesystems gibt. Darüber hinaus stellen das Festhalten an historisch aufgenommenen Daten und tradierte religiöse und gesellschaftliche Gruppenzuordnungen in der indischen Gesellschaft zusätzliche Herausforderungen. Keinesfalls darf unter dem Vorwand eines notwendigen Identitätsmanagements dabei die Privatheit generell zur Disposition stehen. Vielmehr ist eine angemessene Privatheit die Grundlage zur Vermeidung von massiven sozialen und gesellschaftlichen Umbrüchen und den damit verbundenen wirtschaftlichen Nachteilen.

Auch wirtschaftliche Einflussfaktoren und Rahmenbedingungen spielen eine erhebliche Rolle. Fast täglich überschlagen sich die wirtschaftlichen Prognosen für eine der größten Volkswirtschaften der Welt. Der digitale Wachstumsmarkt in Indien scheint unermesslich – aktuell nutzen etwa 300 Millionen Inder das Internet, mehr als 200 Millionen davon über mobile Geräte. In drei Jahren soll bereits jeder zweite Inder online sein und die gesamte „digitale Ökonomie" Indiens auf 200 Milliarden Dollar wachsen: „we are adding five million new users a month and that should take the

user base to 500 million by 2018-19."[3] Im Gegensatz zu Ländern wie China oder Russland ist der indische digitale Markt stark von US-amerikanischen Anbietern beherrscht. Google ist unantastbarer Marktführer bei den meisten werbefinanzierten Produkten, inklusive Suche, Video- und E-Mail-Services. 92 Millionen sind inzwischen im indischen Facebook und 20 Millionen auf Twitter.

3 Der indische Weg

Um die spezifischen Ausprägungen, Herausforderungen und Problemlagen der Digitalisierung in Indien besser zu verstehen, ist ein differenzierter Blick auf die kulturellen und gesellschaftlichen Realitäten Indiens notwendig. Das Bild Indiens erscheint als eine Verbindung von anscheinend ungleichen, aber artverwandten Faktoren, komponiert aus diversen Sprachen und Denkbildern, die Ausdruck sowohl lokaler Momente als auch eingewobener globaler Elemente sind. Geprägt ist Indien heute einerseits durch eine enorme (Wachstums-)Dynamik, die alle Bereiche des Lebens in Indien umfasst, andererseits durch eingeschriebene kulturell-gesellschaftliche Kodizes, zusammengehalten durch die Sprach-Schimäre Hindi-Englisch.

3.1 Modernisierung und Digitalisierung

Für die Digitalisierung der indischen Gesellschaft sind zwei Faktoren wesentlich: a) die Anfang der 90er Jahre als Reaktion auf die veränderte globale Lage eingeleitete wirtschaftliche Liberalisierung, die das heutige IT-Zentrum Bengaluru am radikalsten umgesetzt hat und b) die massive Urbanisierung Indiens, die spätestens mit der Jawaharlal Nehru National Urban Renewal Mission (JNNURM)[4] im Jahre 2005 auch die nationale Politik vom ruralen auf den urbanen Raum verschoben hat.

---

3 Rajan Anandan, Managing Director von Google India, s. http://articles.economictimes.indiatimes.com/2015-02-26/news/59542005_1_internet-economy-internet-growth-google-india.

4 Die Jawaharlal Nehru National Urban Renewal Mission ist ein großes staatliches Stadtentwicklungsprogramm, für welches das Stadtentwicklungsministerium verantwortlich ist. Es markiert den sichtbaren Wechsel stark rural ausgerichteter Politik

Diese beiden Faktoren sind auch insofern von hoher Bedeutung, als die Digitalisierung der indischen Gesellschaft nicht losgelöst von anderen Prozessen und Entwicklungen läuft und somit die Frage nach der digitalen Ausgestaltung, etwa in Bezug auf den Datenschutz, in Indien vor allem eine sozial-gesellschaftliche Frage ist und daher nicht rein wirtschaftlich betrachten werden darf. Das bedeutet zuvorderst, dass es ganz wesentlich um Zugangsmöglichkeiten innerhalb der Gesellschaft geht, verstanden hier im Sinn des Abbaus der starken sozialen und religiösen Barrieren. Denn trotz der quantitativ beeindruckenden Zahlen des digitalen Marktes darf nicht übersehen werden, dass heute noch immer 60% der Bewohner Indiens nicht an diesem teilhaben, während ihre persönlichen Daten, wo immer es möglich ist, nicht nur gesammelt und verarbeitet werden, sondern auch Grundlage politischer und wirtschaftlicher Entscheidungen sind. Da diese Entscheidungen unmittelbare Auswirkungen auch auf diejenigen Bewohner haben, die auf der falschen Seite der digitalen Spaltung leben, ergibt sich ein Ungleichgewicht mit erheblicher Sprengkraft.

3.2 Rudimentärer Datenschutz

Auf der anderen Seite ist die faktische Realität in Indien längst eine Mixtur aus sich verändernden Lebensrealitäten und ihrer digitalen Teilabbildung, wobei sich immense Unterschiede zwischen den ruralen und urbanen Räumen zeigen. Die Gleichzeitigkeit dieser unterschiedlichen Figuren aus faktischer Umwelt und Digitalität führt jedoch zunehmend in ein gesellschaftliches Dilemma. Denn Privatheit und Datenschutz sind aus vielerlei Gründen wenig bis nicht vorhanden. Stattdessen ist die „Selbstveröffentlichung“, beziehungsweise das gezielte digitale (Eigen-)marketing mindestens in Zentren wie Bengaluru nicht nur ein wachendes Phänomen, sondern gerade aufgrund des wirtschaftlichen Drucks auch ein deutlicher faktischer Zwang für jeden Entrepreneur. Hier wiederum zeigt sich das gesellschaftlich höchst divergierende Verständnis zwischen Privatheit und Öffentlichkeit. Vor dem Hintergrund, dass 30% der indischen Bevölkerung

---

hin zu Strategien der Urbanisierung. Mit umgerechnet über 20 Milliarden US-Dollar hat es zum Ziel, die Lebensqualität und die Infrastruktur in urbanen Räumen zu verbessern, s. http://jnnurmmis.nic.in/jnnurm_hupa/index.html.

unter der Armutsgrenze leben,[5] die Analphabetenrate 35% beträgt und – insbesondere in urbanen Räumen – informelle Siedlungsstrukturen zunehmen (oft einhergehend mit prekären Einkommenssituationen), ist der semi-private Raum wesentliche Grundlage, um gemeinschaftlich Platz zu nutzen. Eine eindeutige Trennung von öffentlichem und privatem Raum ist in Indien somit typischerweise nicht vorhanden.

Es verwundert somit nicht, dass es bis heute in Indien nur wenige explizite Regelungen zu Privatheit und Datenschutz gibt, die überdies bislang noch weit von europäischen Standards entfernt sind.[6] Dies liegt auch begründet in der starren patriarchalen Gesellschaftsstruktur, die sich einerseits auf tradierte religiöse Kodizes (Kastensystem) stützt, andererseits aber – insbesondere durch die Kolonialgeschichte – starke soziale Unterschiede beinhaltet. Insbesondere letzteres manifestiert sich zunehmend gerade im urbanen Raum durch eine „neue Mittelschicht" und deren (ökonomischen) Infragestellung tradierter Formen. Da es selbst in der schnell wachsenden asiatischen Volkswirtschaft Indiens nicht gelungen ist, genügend Arbeitsplätze zur Aufnahme des steigenden Arbeitskräftepotenzials zu schaffen, ist der informelle Sektor nach wie vor sehr groß – und damit auch weitgehend außerhalb staatlicher Regulierung.[7]

3.3 Identitätspapiere im föderalen System

Indien ist ein föderaler Staat. Dem föderalistischen Prinzip setzt die Verfassung jedoch eine starke Zentralgewalt, die Indische Union, entgegen. Dieser „Föderalismus von oben" entstand 1947 wesentlich aus der im Zusammenhang mit der Loslösung vom Vereinigten Königreich erkannten Notwendigkeit, einen starken Zentralstaat zur Wahrung der nationalen Einheit zu schaffen. Mit der 1992 verfassungsrechtlich geregelten kommunalen Selbstverwaltung sowie der politischen Ausrichtung auf die urbanen Zentren (JNNURM)[8] 2005 ist in jüngerer Zeit allerdings eine Kompetenz-

---

5 http://www.zeit.de/gesellschaft/zeitgeschehen/2014-07/indien-armutsgrenze-bericht-hilfsprogramme.

6 Zum Datenschutz in Indien s. näher Stauder 2014: 188 ff.; Perry4Law 2014; zu den Problemen in Bezug auf Twitter s. Privacy Laws In India And Privacy Rules And Regulations In India 2015.

7 Chen und Doana 2008.

8 S. Fn. 4.

zunahme der Regionen und der Staaten zu notieren. Dabei zeigt sich, dass die behördlichen Kompetenzen oftmals überlappen und ein hohes Governance-Problem offenbaren. Zudem weist Indien eine hohe Korruption auf (38 Punkte auf dem Corruption Perceptions Index von Transparancy International in 2015).[9]

Die graphische Darstellung der verschiedene Identity Cards in Indien, deren diverse Kompetenzen, sowie die Langwierigkeit der Beantragung zeigen gut das Dilemma in einem Land, in dem bis heute jeder vierte Bürger keinerlei offizielle Papiere besitzt, um seine Identität schriftlich zu belegen. Dies entspricht fast der Gesamtbevölkerung der Europäischen Union.

Hinzu kommt, dass Indien in vielen sozialen Bereichen – insbesondere der Armutsbekämpfung – eine lange Tradition ausländischer Institutionen aufweist, die finanzielle Hilfen und Programme installiert haben und betreiben. Dies führt zeitgleich zu einem Machtverlust und folgendem Kompetenzverlust der indischen Stellen in diesen Kerngebieten staatlicher Verwaltung. Überdies zeigt sich zunehmend, dass im Rahmen globaler Standardisierungsbestrebungen oftmals spezifische soziale und kulturelle Fragen keine Berücksichtigung finden, indem beispielsweise Informalität nicht abgedeckt werden kann und somit wesentliche Gestaltungsmöglichkeiten schlicht unmöglich gemacht werden.

9 http://www.transparency.org/country#IND.

Dokument	Ausgabestelle	Grund	Beantragungszeit	Reale Wartezeit	Anmerkung
Führer-schein	Regionale Trans-port Offices	Dokument zum Nachweis der Fahrerlaubnis	2 Tage	2 Tage – 2 Wochen	Der Führerschein wird nur regional ausgegeben und ist meistens auch nur im jeweiligen Staat gültig. Einige Staaten haben bereits den E-Führerschein eingeführt, der den Fingerabdruck beinhaltet.
Pan Card	Finanzministerium	Die Permanent Account Number ist zwingend für Finanztrans-aktionen und die Steuer	15 Tage / 5 Tage (online)	3 – 5 Wochen	Seit 2011 wird eine elektronisch lesbare Karte ausgegeben. Kritik v.a., da Karte lesbar für private Institutionen und gespeicherte Informationen alle Daten zum Finanzstatus enthalten.
Pass	Außenministerium	Reisen ins Ausland	3 Tage	3 Tage – 8 Wochen	Der E-Pass ist derzeit in Entwicklung und soll 2016 eingeführt werden.
Aadhaar	Unique Identification Authority of India (UIDAI)	Einheitliche Identifikationsnummer	60 – 90 Tage	3 Monate und mehr	Stark kritisiertes, verfassungsrechtlich umstrittenes Projekt, das zudem eine Datenbank inkl. biometrischer Daten anlegt.
Ration Card	Landesregierungen	Identifikationskarte zur Erhaltung von Hilfsmitteln	10 Tage	6 Monate – 2 Jahre	Höchst ineffiziente Karte, da viele faktisch keine Karte bekommen (u.a. aufgrund der langen Wartezeit) und viele gefälschte Karten im Umlauf sind. Eine E-Ration Card existiert, kann aber nur beantragt werden, wenn man bei Aadhaar registriert ist.
Voter ID	Nationale Wahl-kommission	Nachweis der Identität bei Wahlen	10 Tage	6 Monate – 2 Jahre	Trotz Besitz einer Karte ist diese oft ungültig, wenn man nicht im Wahlregister gelistet ist. Zudem existieren zahlreiche Fälschungen.

Tab. 1: Indiens Identitätsdokumente, by MOD Institute[10]

3.4 Identitätsmanagement als Voraussetzung von Inklusion

2009 hat die indische Regierung das Programm Aadhaar eingeführt. Unter der Unique Identification Authority of India (UIDAI) hat dieses ehrgeizige und weltweit größte Datenmanagementprogramm[11] zum Ziel, die biometrischen und demographischen Angaben aller Einwohner zu erfassen und in einer zentralen Datenbank zu sammeln. Jeder erfasste Einwohner bekommt eine 12-stellige eindeutige Identifikationsnummer namens Aadhaar. Gesammelt werden alle zehn Fingerabdrücke, sowie zusätzlich ein Iris-Scan. Zudem werden bei der Registrierung Name, Geschlecht, Wohnort und Alter angegeben. Die Registrierung ist offiziell freiwillig. Faktisch sind jedoch zahlreiche Zugänge zu staatlichen und privaten Transaktionen abhängig von einer Aadhaar-Registrierung, obwohl die Registrierung umgerechnet drei Euro kostet und damit für viele Bürgerinnen und Bürger nicht bezahlbar ist. Zudem wurde die Freiwilligkeit durch die 2011 durchgeführte verpflichtende Volkszählung konterkariert, deren Daten ebenfalls in der zentralen Datenbank gesammelt werden. Die Kritik an dem Programm ist vielfältig; vor allem die Sicherheit der zentralen Datenbank ist fraglich. Mit der im September 2013 gefällten Entscheidung des obersten Gerichtshofs in Indien, dass niemand aufgrund der Nicht-Registrierung einen Nachteil erleiden darf („no person should suffer for not getting Aadhaar"),[12] ist der Zugang zu staatlichen Hilfsleistungen losgelöst von einer Registrierung. Die weitere Ausgestaltung des Programms liegt nun wieder beim indischen Parlament. Der wohl größte Gewinner des Projekts ist die IT-Branche. Der UIDAI-Vorsitzende Nandan Nilekani ist ehemaliger Geschäftsführer von Infosys, einem der größten IT-Unternehmen Indiens, das maßgeblich an der Entwicklung von Aadhaar beteiligt ist. Neben diesen problematischen Verflechtungen kritisieren zivilgesellschaftliche Gruppen (beispielsweise Citizens Forum for Civil Liberties oder Indian Social Action Forum, INSAF) den fehlenden Datenschutz. Dies betrifft vor allem drei zentrale Momente, nämlich das mögliche Profiling, die intransparente

10 S.a. http://www.dailymail.co.uk/indiahome/indianews/article-2297714/Indias-identity-crisis-Between-Aadhaar-passport-PAN-NPR-struggling-prove-identities.html.

11 Jayashankar und Ramnath 2010.

12 Der Supreme Court of India hatte dies 2013 als interim order im Verfahren über die Writ Petition (Civil) No. 494 of 2012 beschlossen. Die interim order wurde 2015 bestätigt und präzisiert, s. https://assets.documentcloud.org/documents/2270729/sc-aadhaar-order.pdf.

Datensammlung und Verknüpfung der Daten sowie den Zugang zur Datenbank, deren Abruf auch privaten Akteuren (wie beispielsweise Banken) gestattet ist.

Im Jahr 2013 hat die indische Regierung das 12-Jahres-Programm Rajiv Awas Yojana (RAY) aufgelegt, welches das ehrgeizige Ziel der Slum-Free-Cities bis 2015 verfolgt. Grundlegende Schwerpunkte sind u.a. die Bereitstellung von Basisinfrastrukturen, die Verbesserung von Zugängen zu Wohnraum oder die Schaffung des Zugangs zu institutionellen Finanzierungsmöglichkeiten. Das Programm nimmt sich zwar einem grundlegenden Problem an, es offenbart jedoch im Hinblick auf die in diesem Kapitel behandelten Punkte wesentliche Fragen, allen voran Privatheit und Identität im Hinblick auf die gesellschaftlich-soziale Dimension. Eine effektive staatliche Daseinsvorsorge benötigt eine hinreichende Datenbasis über die Lebensrealitäten der Betroffenen und läuft genau deshalb Gefahr, tief in deren Persönlichkeitssphären einzudringen. Dies zeigt sich hier sehr deutlich: Eine Voraussetzung für das Gelingen im Potpourri der Maßnahmen, die auf eine Slum-freie Stadt zielen, ist eben nicht nur die genaue Sammlung der nur unzureichend vorhandenen Daten (einschließlich finanzieller, kultureller und sozialer Beziehungen), sondern auch eine anonymisierte Kartographierung der Viertel. Das Dilemma der notwendigen Datengrundlage, um – in diesem Fall – staatliche Leistungen nicht nur überhaupt zu ermöglichen, sondern sie auch wirkungsvoll an ihre jeweiligen Adressaten leiten zu können, ist unbestritten. Die Kehrseite jedoch ist, dass informelle Strukturen (auch aufgrund ökonomischen Drucks) wenig Chancen haben, ihre Identitäten zu wahren und illegal wohnende Menschen unmittelbar in ihrer Existenz bedroht sind. Vor dem Hintergrund, dass beispielsweise Religion und Kastenzugehörigkeit registriert werden und über den Zugang zum Gemeinwesen wesentlich entscheiden, ist die Umsetzung datenschutzrechtlicher Prinzipien für die Erhebung, Verarbeitung und Nutzung derartiger sensibler Daten von besonderer Bedeutung.

Indien steht insoweit zwischen zwei Polen: einerseits die globalen Marktanforderungen, Interessen und sicherheitsrelevanten Fragen, andererseits die nationalen Realitäten und hier insbesondere die Anforderung, die großen sozialen Probleme lösen zu wollen und zu müssen. Die zeitgleiche rapide Urbanisierung und die sich immens verschärfende soziale Schere erschweren dies zunehmend. Wachsende Regulierungs- und Standardisierungstendenz werden durch die oben benannten Governanceprobleme und eine steigende Rechtsunsicherheit ad absurdum geführt. Die Digitalisierung erscheint hier als ein Rettungsanker. Durch das weitgehen-

de Fehlen inklusiver staatlicher Institutionen führen die einzelnen Digitalisierungsstrategien jedoch kaum zu einer tatsächlichen Ermöglichung der Teilhabe, sondern die sozialen Unterschiede werden im Gegenteil rapide verstärkt. Dass in Indien traditionell informelle Abläufe und dezentrale Strukturen wichtige Beiträge zur Lösung sozialer Herausforderungen liefern, ist ein gewaltiges Kapital, welches auch bei den neuen Herausforderungen der Einführung von IT-Infrastrukturen im Sinne sowohl des Einzelnen als auch des indischen Gemeinwesens genutzt werden sollte. Dazu im Gegensatz steht der zunehmende Einfluss globaler Player wie Google oder Facebook, die gerade in Indien einen fruchtbaren Boden hinsichtlich der schleichenden Übernahme staatlicher Funktionen finden.

3.5 Sicherheitsinteressen

Ein nicht wegzudiskutierendes Problem der inneren Sicherheit Indiens sind die religiösen Gegensätze und ethnischen Konflikte. Die damit verbundene, weiter zunehmende Radikalisierung größerer Bevölkerungsgruppen führt zu Forderungen nach neuen Sicherheitsmaßnahmen und schlägt sich wesentlich in Argumenten gegen Privatheit und Datenschutz nieder, mehr noch: Sie fungiert als Rechtfertigung jeglicher Sammlung von Daten. In diesem Zusammenhang laufen momentan zwei verfassungsrechtlich sehr umstrittene Projekte in Indien.

Das erste Programm, genannt Central Monitoring Programme (CMS), ist ein elektronisches Datensuch- und Überwachungssystem, das vom Centre for Development of Telematics (C-DOT), einem staatlichen Technologieentwicklungszentrum, installiert wurde und mittels Telecom Enforcement Resource and Monitoring (TERM) betrieben wird.[13] Es ermöglicht der Exekutive einen zentralen Zugang zur indischen Telekommunikationsinfrastruktur und bietet dabei die Möglichkeit, mobile und stationäre Anrufe, VoIP, E-Mails, SMS und MMS in Echtzeit abzuhören und mitzuschneiden, sowie eine Geodatenlokalisierung der Kommunikationsteilnehmer vorzunehmen. Telekommunikationsprovider in Indien sind seit 2014 gesetzlich verpflichtet, alle Verbindungsdaten offenzulegen.

Das zweite Programm ist das NEtwork TRaffic Analysis (NETRA), entwickelt durch das Centre for Artificial Intelligence and Robotics

13 Näher Centre for Internet and Society 2013.

(CAIR).[14] Anwender sind das Intelligence Centre und der Research and Analysis Wing (RAW). Das Programm analysiert den gesamten indischen Internetverkehr.

3.6 Homogenität und Individualität in der Stadt der Zukunft

Quasi über diesen Entwicklungen schwebt die Vision der „Smart City", also die digitale technologiebasierte urbane Entwicklung. In dieser liegt der postulierte Rettungsanker für die Probleme der indischen Moderne, nicht erst seit dem Programm „100 New Smart Cities Programm" von Premierminister Narenda Modi.[15] Dahinter liegt vor allem der Glauben an Modelle von Messbarkeit und technologischen Anwendungen auf der Basis von Standardisierung und Vereinfachung.

„Smart City wird es in hundert Jahren in Indien nicht geben – wir haben andere Probleme. Vor einiger Zeit trat ein Vertreter einer Firma an uns heran mit dem Versprechen beim Kauf ihrer Software enorme Einsparungen im Energiehaushalt verbuchen zu können. Ich habe ihm geantwortet dass es preiswerter ist, wenn wir jemanden einstellen, der sich darum kümmert, vergessene Lampen einfach auszuschalten."[16]

Das Zitat karikiert die Situation in Indien und verdeutlicht die existierende gegenwärtige Situation. Auch der oben genannte Diskurs zur Informalität entspricht diesen vereinfachten globalen Blaupausen, die die spezifisch indische Situation nicht abdecken können. Die wesentliche Frage ist jedoch, wie viel Sichtbarkeit die Stadt, beziehungsweise die Gesellschaft vertragen kann. Vor dem Hintergrund der oben gezeigten sozialen Verhältnisse offenbart sich hierin das grundlegende Dilemma zwischen Identitätsmanagement, Privatheit und Datenschutz: „Es ist lächerlich, zu glauben, es gebe eine technologische Lösung für den sozialen Ausgrenzungsprozess."[17]

---

14 Das Centre for Artificial Intelligence and Robotics (CAIR) ist der Forschungsarm der dem Verteidigungsministerium unterstellten Defence Research & Development Organization (DRDO). Ihre Forschung und Entwicklung umfassen sichere Kommunikation, technische Infrastrukturen und intelligente Systeme.

15 Vgl. http://smartcities.gov.in/.

16 Randnotiz, Besuch im III-T, Bangalore, Flurgespräch im April 2014.

17 So die indische Ökonomin Javati Ghosh in einem Interview im Jahre 2012, s. Die ZEIT 50/2012, http://www.zeit.de/2012/50/Indien-Armut-Jayati-Ghosh.

4 Ausblick: Zivilgesellschaftliche Strategien und Governance-Defizite

Die Debatte in Indien, obwohl sie „nur“ von einer kleinen Gruppe von Aktivisten initiiert wurde, vergrößert sich derzeit – gerade aufgrund der sozialen Dimensionen – um Bürgerrechtsgruppen und soziale NGOs. Bemerkenswert ist sicherlich der Report des Parliamentary Standing Committee on Information Technology, das Anfang 2014 in seinem Report „Cyber-Crime, Cyber Security and Right to Privacy“[18] die geringen Privatheits-Rechte anprangerte. Denn das im Juni 2011 verabschiedete Programm ist noch immer nicht in Kraft. Letztlich ist Datenschutz in Indien derzeit wesentlich abhängig von den Akteuren – und da zeigt sich, dass abseits existierender Regelungen sehr wohl Datenschutzmechanismen angewandt werden. Drei Beispiele illustrieren dies: Der Collective Research Initiatives Trust (CRIT), ein urbanes Forschungsinstitut aus Mumbai, dokumentiert Vieles in fiktionalen Geschichten, da der Einblick in die resilienten Strategien einen elementaren Wissensvorsprung darstellt, der geschützt werden muss.[19] Wie notwendig Privatheit ist, zeigen vor allem Beispiele, die sich gesellschaftlicher Tabuthemen annehmen. Das Portal 1to1help startete ursprünglich mit einem psychotherapeutischen Angebot an Unternehmensmitarbeiter. Dieses Angebot funktionierte jedoch erst mit dem Launch einer Website, die anonyme Anfrage ermöglicht.[20] Nextbengaluru oder Fields of View, beides NGOs in Bengaluru, folgen strengen Datenschutz- und Creative Commons-Modellen in ihrer Arbeit. Aus Sicht der Nichtregierungsorganisationen ist dies wesentliche Grundlage, um Partizipation und Beteiligung zu ermöglichen.[21] „The biggest problem we need to understand is that urbanity is mostly communicated in numbers, but to be honest, all data – big or small – is just a set of algorithms of uncertainty.“[22]

In Indien verdeutlichen sich somit die immensen Herausforderungen eines staatlichen Systems im Hinblick auf die Digitalisierung, das trotz vieler Bemühungen ein hohes Governancedefizit aufweist und bisher keinen ausreichenden inklusiven Zugang für alle Bevölkerungsgruppen ermög-

---

18 S. Standing Committee on Information Technology 2014; näher Dalal 2014.
19 Vgl. CRIT Mumbai, www.crit.in.
20 http://1to1help.net/.
21 Vgl. von Damm et al. 2015; Saunders und Baeck 2015.
22 Bharat Palavalli, Interview zum Thema “What is urban? Where do we go from here?”, in: von Damm et al. 2014: 21

licht hat. Eine Lösung dieser Probleme setzt voraus, dass die notwendige Garantie von Privatheit und Datenschutz als Grundlage eines nicht nur in sozialer, sondern auch in ökonomischer Hinsicht angemessenen Identitätsmanagements verstanden werden muss. Dieser Lösungsansatz ist auch für weitere technologie-basierte Modelle wie die Vision der Smart City anwendbar, die zuvorderst den nachhaltigen Zugang des Einzelnen zum Gemeinwesen garantieren müssen.

Literatur

Centre for Internet and Society (2013): *India's 'Big Brother': The Central Monitoring System (CMS)*, http://cis-india.org/internet-governance/blog/indias-big-brother-the-central-monitoring-system.

Chen, Martha and *Doana, Donna* (2008): *Informality in South Asia: A Review. Wiego Working Paper No 4*, http://wiego.org/publications/informality-south-asia-review-0.

Dalal, Praveen (2014), *Parliamentary Committee Slams Indian Government For Poor Privacy Laws In India*, http://www.electroniccourts.in/privacylawsindia/?p=13.

von Damm Tile, Ewald Markus, Fenk Anne-Katrin und *Lynen Leona (Hrsg.)* (2014): *Crowdsourcing the City*, Berlin, http://blog.goethe.de/weltstadt/uploads/140417_BANGALORE_RZ_print.pdf.

von Damm Tile, Ewald Markus und *Fenk Anne-Katrin* (2015): *People's Vision on Future Shanthinagar*, MOD Institute, Bengaluru, http://www.mod.org.in/mod/out-now-peoples-vision-on-future-shanthinagar/.

Eliot, T.S. (1934): *The Rock*, London: Faber & Faber.

Jayashankar, Mitu and *Ramnath, N.S. (*2010): „UIDAI: Inside the World's Largest Data Management Project", in: *Forbes India*, http://forbesindia.com/article/big-bet/uidai-inside-the-worlds-largest-data-management-project/19632/1.

Perry4Law (2014): *Data Protection Laws In India And Privacy Rights In India*, http://ptlb.in/clpic/wp-content/uploads/2014/01/Data-Protection-Laws-In-India-And-Privacy-Rights-In-India.pdf.

Privacy Laws In India And Privacy Rules And Regulations In India (2015): *Twitter Is Now Censoring Critical And Dissenting Digital India Related Tweets*, http://www.electroniccourts.in/privacylawsindia/?p=146.

Saunders, Tom und *Baeck, Peter* (2015): *Rethinking Smart Cities from the Ground Up*, Nesta, http://www.nesta.org.uk/sites/default/files/rethinking_smart_cities_from_the_ground_up_2015.pdf.

Standing Committee on Information Technology (2014): *Cyber-Crime, Cyber Security and Right to Privacy. Fifty-Second Report*, http://164.100.47.134/lsscommittee/Information%20Technology/15_Information_Technology_52.pdf.

Stauder, Clemens (2014): „Indien – Drittstaat mit angemessenem Datenschutzniveau? Das indische Datenschutzrecht im Überblick", in: *Zeitschrift für Datenschutz*, 188-192.

Zahlungsbereitschaft für Föderiertes Identitätsmanagement

Heiko Roßnagel / Jan Zibuschka / Oliver Hinz/ Jan Muntermann[1]

1 Einleitung

Zuverlässige Authentisierung, also die Feststellung dass ein Nutzer tatsächlich einer einem Dienstanbieter bekannten Identität entspricht, ist eine Grundvoraussetzung für E-Commerce und andere Transaktionsdienste im Web (Schläger et al. 2006). Bisher sind Passwörter die dominierende Authentisierungsmethode. Sie sind einfach nutzbar und erfordern keine teure Hard- oder Software auf der Client-Seite (Mannan und Van Oorschot 2007). Andererseits führen sie auch zu zahlreichen Problemen, wie dem aufwendigen Passwortmanagement (Recordon und Reed 2006), der Wiederverwendung von Passwörtern (Ives et al. 2004), sowie weiteren Sicherheitsproblemen (Neumann 1994). Föderiertes Identitätsmanagement (FIM) stellt eine vielversprechende Technologie für die Authentisierung von Nutzern sowie die Verteilung von Identitätsinformationen über Organisationsgrenzen dar (Maler und Reed 2008). Es bietet zudem die Möglichkeit, ein organisationsübergreifendes Single-sign-on bereitzustellen, das eine einheitliche Authentisierungs- und Authorisierungsinfrastruktur nutzt und somit die Notwendigkeit mehrerer unterschiedlicher Passwörter eliminiert. In den letzten Jahren wurden zahlreiche unterschiedliche Lösungen für FIM entwickelt, die sich unterschiedlich erfolgreich am Markt etabliert haben (Hühnlein et al. 2010). Verschiedene Autoren haben ganz unterschiedliche Gründe für diesen uneinheitlichen Markterfolg identifiziert, wie beispielsweise Defizite bei Sicherheit und Privatsphärenschutz (Kormann und Rubin 2000); (Hansen et al. 2004) oder schlechte Bedienbarkeit (Dhamija und Dusseault 2008). Dabei lag der Fokus auf der Angebotsperspektive. Bisher gibt es unseres Wissens nach keine empirischen Untersuchungen, die diese Thesen aus der Bedarfsperspektive validiert haben. Ziel dieser Arbeit ist es, diese Lücke zu schließen. Dieser Beitrag be-

1 Dieser Beitrag ist eine gekürzte Übersetzung von Roßnagel et al. 2014. Teile davon sind bereits in Zibuschka 2014 erschienen.

schäftigt sich mit der individuellen Zahlungsbereitschaft für föderiertes Identitätsmanagement. Dazu führen wir eine Choice-Based-Conjoint-Analyse (CBC) durch, mit der wir Nutzerpräferenzen messen. Auf Basis einer repräsentativen Stichprobe der deutschen Internetbevölkerung messen wir die Auswirkungen von verschiedenen Designentscheidungen auf die Zahlungsbereitschaft der Nutzer.

2 Verwandte Arbeiten

Es gibt zahlreiche Untersuchungen zu Web-Identitätsmanagementlösungen. Dabei wurden verschiedene Faktoren für den Markterfolg solcher Lösungen identifiziert:

- Zahlreiche Autoren haben den Grad des Privatsphärenschutz als einen entscheidenden Faktor beschrieben (Acquisti 2008; Josang et al. 2007). So schlagen Hansen et al. (2004) ein 'privacy-enhancing identity management' vor, das maximale technische Privacy-Garantien bietet.
- Sicherheit wird ebenfalls häufig als wichtiger Erfolgsfaktor genannt (Dhamija und Dusseault 2008; Krolo et al. 2009). So führen beispielsweise Fu et al. (2001) den Misserfolg von Microsoft Passport auf existierende Sicherheitslücken und den damit verbundenen Vertrauensverlust zurück.
- Ein weiterer in der Literatur oft genannter Erfolgsfaktor ist die Bedienbarkeit der Lösung (Dhamija und Dusseault 2008; Josang et al. 2007). Es besteht ein Konsens, dass es aufgrund hoher Komplexität von Identitätsmanagementsystemen, die durch zahlreiche Sicherheits- und Privatsphärenschutzanforderungen entsteht, sehr schwierig ist, einfach zu bedienende Nutzerschnittstellen zu entwerfen.
- Auch Interoperabilität wird häufig als kritischer Erfolgsfaktor genannt (Bhatti et al. 2007; Backhouse et al. 2003). Durch die Interoperabilität eines Systems bestimmt sich auch die Breite des Einsatzgebiets, wodurch die wahrgenommene Nützlichkeit für den Nutzer beeinflusst wird.

Die hier genannten Faktoren bilden natürlich keine vollständige Liste aller Möglichkeiten. Sie sind aber diejenigen, die in der Literatur am häufigsten genannt werden. Daher werden wir uns im Folgenden auch auf diese Faktoren konzentrieren.

Während die meisten Forschungsarbeiten einzelne Erfolgsfaktoren isoliert voneinander diskutieren, gibt es auch einige Studien, die sich mit der Diffusion von Identitätsmanagementsystemen beschäftigen (Hühnlein et al. 2010; Zibuschka und Roßnagel 2008) beschreiben die zugrundeliegenden Netzwerkeffekte, die von verteilten Single-sign-on-Architekturen ausgehen, bei denen die Nützlichkeit für die Nutzer umso stärker steigt, je mehr Anbieter kompatible Dienste anbieten. In (Landau und Moore 2011) wurden aktuelle Trends untersucht, insbesondere die Verbreitung von föderierten Identitätsmanagementsystemen bei Dienstanbietern.

In der Studie, die unserem Beitrag am nächsten kommt, haben Mueller et al. (2006) Nutzerpräferenzen und Zahlungsbereitschaften für FIM in Südkorea untersucht. Im Hinblick auf Sicherheit und Privatsphärenschutz wurden die generischen Attribute "security level" und "private information" verwendet. Unser Beitrag erweitert die Arbeiten von Mueller et al. (2006) um drei Aspekte:[2]

(1) Da wir uns auf den deutschen Markt konzentrieren, dürften kulturelle Unterschiede zu Südkorea zu erwarten sein;
(2) der Markt für FIM hat sich in den letzten Jahren dynamisch entwickelt und neue Technologien und Anwendungen hervorgebracht; und
(3) fokussieren wir uns auf Charakteristika, die in frühen Phasen des Entwicklungsprozesses (Chapman et al. 2008) angewandt werden können. Generische Konstrukte wie das von Mueller et al. (2006) verwendete „security level" erscheinen da eher kontraproduktiv zu sein.

3 Forschungsansatz

Eine CBC wird benutzt, um empirische Daten zu Nutzerentscheidungen zu erheben. Auf dieser empirischen Basis werden Teilnutzenwerte mittels einer hierarchischen Bayes-Analyse ermittelt, deren Ergebnisse in Zahlungsbereitschaften zurücktransformiert werden. In einem zweiten Schritt wird auf Basis psychografischer Daten eine Segmentierung der potentiellen Kunden vorgenommen. So werden durch die Erhebung von Teilnutzenwerten für IdMS mit verschiedenen Attributsausprägungen die wesent-

2 Für eine ausführliche Diskussion der Arbeit von Mueller et al. (2006) siehe Roßnagel et al. 2014.

lichen Präferenzen ermittelt, die verschiedene Kundengruppen an IdMS stellen.

Auf Basis einer CBC ist es möglich, die attributbasierten Teilnutzenwerte, den Preisparameter sowie den Parameter für die "Nicht-Kauf"-Option (bei welcher der Nutzer unabhängig von der Ausprägung keines der IdMS nutzen will) zu bestimmen:

$$P_{h,i} = \frac{\exp(u_{h,i})}{\exp(u_{h,NP}) + \sum_{i' \in C_a} \exp(u_{h,i'})}$$

($h \in H$, $i \in I$), wobei

$P_{h,i}$:Wahrscheinlichkeit, dass Kunde h Produkt i wählt

$u_{h,i}$:Nutzen von Produkt i für Kunden h

$u_{h,NP}$:Nutzen der "Nicht-Kauf"-Option für Kunden h

C_a:Indexmenge der Alternativen in Auswahlmenge a ($C_a \subseteq I$)

H:Indexmenge der Kunden

I:Indexmenge der Produkte (ohne " Nicht-Kauf "-Option)

Die Wahrscheinlichkeit, dass ein Kunde ein Produkt wählt, hängt vom Nutzen des Produktes i für den Kunden h, $u_{h,i}$, ab, welcher der Summe der Attribut-basierten Teilnutzen und dem Teilnutzen des Preises entspricht:

$$u_{h,i} = \sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} + \beta_{h,price} \cdot p_i$$

($h \in H$, $i \in I$), wobei

$\beta_{h,j,m}$: Parameter der Attributsausprägung m des Attributs j für Nutzer h (Attribut-basierter Teilnutzenwert)

$x_{i,j,m}$: Variable, die angibt, ob Produkt i Niveau m des Attributs j anbietet

$\beta_{h,price}$: Preis-Parameter für Nutzer h

p_i: Preis des Produkts i

M: Indexmenge der Niveaus

J: Indexmenge der Attribute ohne Preis

Die Parameter für die Kunden in H werden mittels eines hierarchischen Bayes (HB)-Modells abgeschätzt. Das HB-Modell hat zwei Ebenen. Zu-

nächst wird auf der höheren Ebene angenommen, dass die Teilnutzenwerte der prospektiven Konsumenten einer multivariaten Normalverteilung entsprechen. Eine solche Verteilung wird durch einen Vektor von Mittelwerten und eine Kovarianzmatrix charakterisiert. Auf der niedrigeren Ebene wird die Annahme getroffen, dass die Entscheidungswahrscheinlichkeit der Benutzer für die Alternativen der Auswahlmenge mittels eines multinomialen Logit-Modells von den Teilnutzenwerten abgeleitet werden kann. HB wurde insbesondere gewählt, da es die flexible Berücksichtigung von Informationen über Modellparameter erlaubt. Darüber hinaus bietet HB die Möglichkeit, individuell spezifische Abschätzungen vorzunehmen und kann die Unsicherheit in diesen Abschätzungen kalkulieren (Gensler et al. 2012). Im vorliegenden Fall eignet sich HB insbesondere, da es eine Abschätzung der Teilnutzenwerte der Attributsausprägungen erlaubt, ohne dafür eine übermäßig große Menge an Antworten zu erfordern. Eine ausführlichere Darstellung von HB findet sich in (Gelman et al. 2003). Durch die Kombination von CBC und HB werden die einzelnen Teilnutzenwerte der verschiedenen IdMS-Attribute und ihrer Ausprägungen ermittelt. Im nächsten Schritt werden diese in monetäre Zahlungsbereitschaften (*willingness to pay*, WTP) transformiert.

Die Zahlungsbereitschaft $WTP_{\mathrm{h,i}}$ für ein Produkt ist definiert als der Preis, bei dem es dem Kunden h gleichgültig ist, ob er das Produkt i erwirbt oder nicht (Moorthy et al. 1997). Der Nutzen des Produkts unter Berücksichtigung des Preises entspricht dann dem Nutzen, es nicht zu kaufen, oder $u_{\mathrm{h,NP}}$. Dieser entspricht wiederum dem Wert der Nicht-Kauf-Option $\beta_{\mathrm{h,NP}}$:

$$\sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} + \beta_{h,\mathrm{price}} \cdot WTP_{h,i} = \beta_{h,\mathrm{NP}}$$

Äquivalenzumformung führt zu:

$$WTP_{h,i} = \frac{1}{\beta_{h,\mathrm{price}}} \cdot \left(\beta_{h,\mathrm{NP}} - \sum_{j \in J} \sum_{m \in M} \beta_{h,j,m} \cdot x_{i,j,m} \right)$$

Nach der ökonomischen Theorie maximieren Konsumenten ihre Konsumentenrente. Daher sollten sie dasjenige IdMS aus dem Auswahlset wählen, für welches diese Konsumentenrente am höchsten ist. Wenn alle Preise höher sind als die relevanten Zahlungsbereitschaften des Benutzers, ist

davon auszugehen, dass dieser die „Nicht-Kauf"-Option wählt, also angibt, er würde keines der Produkte kaufen. Durch Anwendung dieser Konzepte lässt sich die WTP für jedes Produkt *i* jedes Konsumenten *h* ermitteln. Es lassen sich so auch Zahlungsbereitschaften extrapolieren, welche außerhalb des Intervalls der abgefragten Preisniveaus liegen.

Schließlich wird eine Clusteranalyse eingesetzt, um verschiedene Marktsegmente für IdMS zu identifizieren. Als Basis der Ermittlung der relevanten Ähnlichkeitsstrukturen dienen psychografische Informationen über die befragten Konsumenten, insbesondere Charakteristiken wie Risikoaffinität, Vertrauen und Preisbewusstsein. So können die WTP und damit die optimalen Produkte für die verschiedenen Marktsegmente ermittelt werden.

4 Aufbau der Studie

Wie bereits erwähnt, wird eine CBC mit Nicht-Kauf-Option durchgeführt. Die den Nutzern vorgelegten Auswahlmengen (sogenannte Choice Sets) bestehen jeweils aus zwei verschiedenen Produkten sowie der Nicht-Kauf-Option. Da die gewählten Attribute und ihre Ausprägungen kritisch für den Erfolg einer CBC sind (Auty 1995), wurde eine Vorstudie in Form einer Expertenbefragung durchgeführt, die in einer Umfrage mit 216 Antworten validiert wurde, um die für Nutzer relevantesten Attribute von IdMS zu bestimmen. In dieser Vorstudie wurden alle von Mueller et al. (2006) verwendeten Attribute abgefragt, allerdings wurden die Ausprägungen von "Sicherheit" angepasst und durch spezifischere Ausprägungen wie Authentisierungsmethode, Zugangskontrolle oder Zertifizierung ersetzt, da die ursprünglich verwendeten prozentualen Ausprägungen nicht auf das Systemdesign anwendbar sind. Außerdem wurden weitere Attribute einbezogen, etwa Anwendungsbereich als mögliche Alternative für den von Mueller et al. (2006) verwendeten Industriesektor (*'industry sector'*) und Abdeckung (*'coverage of identifier'*) mit Implikationen für den Entwurf. Auf Basis dieser Vorstudie wurden die folgenden drei Attribute ausgewählt (mit Preis als viertem Attribut, um die WTP zu extrapolieren, s. Tabelle 1):

Das erste Attribut ist im Bereich der Sicherheit von IdMS angesiedelt. Die von Nutzern als besonders relevant empfundenen Ausprägungen decken sich weitgehend mit dem Grad der Zertifizierung der im System verarbeiteten Identitäten durch Dritte. IdMS, die übertragene Identitätsinfor-

mationen zertifizieren, werden generell als sicherer angesehen, da mit der Zertifizierung oftmals eine Garantie der Informationen einhergeht. Auch für den Systementwurf ergeben sich klare Implikationen, da Systeme mit Zertifizierung üblicherweise eine stärkere Authentisierung einsetzen, etwa Tokens oder Biometrie, eine Attributsausprägung, die Nutzer ebenfalls als relevant einstuften und die so mit abgedeckt werden kann. In der Vorstudie zeigten sich Zertifizierung und Authentisierungstechnik als die relevantesten Ausprägungen, die zusammen als ungefähr so bedeutsam wahrgenommen wurden wie die Anwendbarkeit des Systems, weshalb das präsentierte Sicherheitsattribut gewählt wurde. Es wurde in folgende drei Ausprägungen gegliedert:

1. **Identitätsattribute von Benutzer:** Der Nutzer gibt seine Identitätsattribute selbst an. Es handelt sich dabei um unbestätigte Behauptungen, die nicht von einer dritten Partei verifiziert werden.
2. **Zertifizierung der Identität:** Die Identitätsattribute werden von einer dritten Partei bestätigt, ohne dass diese Partei eine Haftung für die Echtheit der Attribute übernimmt.
3. **Rechtsverbindliche Zusicherung:** Die Identitätsattribute werden durch eine dritte Partei rechtsverbindlich bestätigt. Die dritte Partei garantiert die Korrektheit der Identitätsattribute.

Da Datenschutz in der IdM-Literatur als kritisches Attribut von IdMS identifiziert wurde, ist es nicht überraschend, dass das zweite verwendete Attribut verschiedene Ausprägungen des Privatsphärenschutzes in IdMS abfragt. Hinsichtlich des Datenschutzes stellte die Vorbefragung fest, dass die Nutzer die für die Verarbeitung der Daten verantwortliche Partei am relevantesten fanden, gefolgt vom Grad der Pseudonymisierung/Anonymisierung, die das System erlaubt. Erneut war die Kombination ungefähr so bedeutsam wie die Abdeckung. Zusammen mit Abdeckung und den beiden Faktoren zur Sicherheit waren dies die fünf gewichtigsten festgestellten Faktoren und deutlich relevanter als beispielsweise Industriesektor aus der Studie von Mueller et al. (2006). Das Attribut Datenschutz hat direkte Auswirkungen auf den Entwurf von IdMS und beeinflusst den Ort der Datenverarbeitung sowie die eingesetzten kryptografischen Verfahren, z.B. anonyme oder attributsbasierte Credentials. Wieder werden drei Ausprägungen vorgesehen:

1. **Identity Provider verwaltet Nutzerdaten:** Die Benutzer hinterlegen ihre Nutzerdaten bei einem Dienstanbieter. Dieser verwaltet diese Nut-

zerdaten und gibt sie nach Anforderung an andere Dienstanbieter weiter.
2. **Nutzer stellt Daten bereit:** Die Daten werden beim Nutzer (Clientseitig) gespeichert. Der Nutzer behält die volle Kontrolle über die Daten und entscheidet jedes Mal selbst, welche Daten an Dienstanbieter weitergegeben werden.
3. **Anonyme Credentials:** Der Benutzer bleibt anonym. Mit Hilfe von anonymen Credentials kann er nachweisen, dass er bestimmte Attribute besitzt (z.B. „ist volljährig"), ohne dass mehrere Zugriffe auf denselben Dienst dadurch verkettbar werden, das heißt, ohne dass er wiedererkannt wird.

Nach der Vorbefragung ist Anwendbarkeit der von Benutzern als am relevantesten empfundene Faktor und erheblich wichtiger als beispielsweise "*coverage of identifier*" oder "*service provider*". Gleichzeitig sind die drei gewählten Ausprägungen mit klaren Implikationen für den Systementwurf verbunden:

1. **Nur nicht-kommerzielles Web:** Das IdM kann nur für nicht-kommerzielle Services genutzt werden. Das System wird nicht von E-Commerce-Anbietern unterstützt.
2. **Web inklusive E-Commerce:** Das System kann sowohl für nichtkommerzielle als auch kommerzielle Dienste genutzt werden.
3. **E-Government, E-Commerce und private Kommunikation:** Das IdM kann für alle Web-basierten Dienste genutzt werden.

Die Benutzbarkeit und andere relevante Attribute von IdMS sind von der spezifischen Implementierung abhängig. Da IdMS also Erfahrungsgüter sind und diese Attribute daher zu (implementierungs-) spezifisch für den Einsatz in der frühen Produktplanung sind (Chapman et al. 2008), wird die Benutzbarkeit nicht abgefragt.

Da auch zur Ermittlung der Nutzerpräferenzen eine differenzierte WTP erhoben werden muss und da IdMS, die über die Grundkonfiguration (1-1-1) hinausgehen, üblicherweise Entgelte für die Bereitstellung und/oder Nutzung von den Endnutzern fordern, werden fünf differenzierte Preisniveaus untersucht, die das im Markt übliche Intervall abdecken: jährlich 2 Euro, 5 Euro, 10 Euro, 20 Euro oder 40 Euro.

Attribut	Attributsausprägung
Sicherheit	• Identitätsattribute von Benutzer • Zertifizierung der Identität • Rechtsverbindliche Zusicherung
Privatsphärenschutz	• IdP verwaltet Nutzerdaten • Nutzer stellt Daten bereit • Anonyme Nutzung von Diensten möglich
Einsatzgebiet	• Nur nicht-kommerzielles Web • Web inklusive E-Commerce • E-Government, E-Commerce und private Kommunikation
Preis	• 2 € pro Jahr • 5 € pro Jahr • 10 € pro Jahr • 20 € pro Jahr • 40 € pro Jahr

Tabelle 1: Untersuchte Attribute von IdMS und deren Ausprägungen

Wichtig für die erfolgreiche Durchführung einer CBC ist die Auswahl eines geeigneten Versuchsplans (Street und Burgess 2007). Die Attributniveaus der Produktalternativen in der CBC werden durch Anwendung eines D-effizienten, teilfaktoriellen Versuchsplans systematisch variiert. Es wurde die Sawtooth Software zur Konstruktion eines D-optimalen (3^3 · 5)-faktoriellen Versuchsplans mit 16 Auswahlmengen verwendet. Diese Art von Versuchsplan ist für ihre hohe Effizienz und flexible Anwendbarkeit für eine große Anzahl von Forschungsansätzen bekannt. Jede Auswahlmenge besteht aus zwei IdMS-Ausprägungen und der Nicht-Kauf-Option, mit der der Nutzer ausdrückt, dass er keines der Systeme einsetzen möchte (s. Abbildung 1). Da der Nutzer den Preis der Systeme mehrmals entrichten muss und gleichzeitig sein SSO-basierter Nutzen sinkt, ist diese Annahme naheliegend.

Es wurde eine Effizienz von 91.29% im Vergleich zum optimalen Versuchsplan festgestellt. Die Beobachtungen von 14 der 16 Auswahlmengen flossen in die abgeschätzte WTP ein, die verbliebenen zwei wurden zur Bestimmung der Voraussagevalidität eingesetzt.

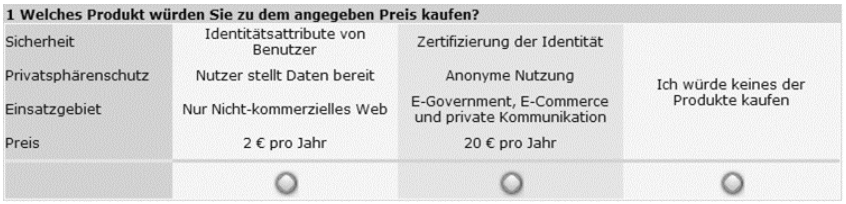

Abbildung 1: Auswahlmenge von Gesamtprodukten in der Umfrage

Conjoint-Analysen beobachten generell prospektive Kunden in hypothetischen Situationen, was theoretisch zu Abweichungen führen kann. Beispielsweise könnten Studienteilnehmer versuchen, den Preis zukünftiger Produkte zu senken, indem sie eine niedrigere Zahlungsbereitschaft vorgeben. Solche Abweichungen sind auch tatsächlich festgestellt worden (Cummings und Taylor 1999). Aktuelle Untersuchungen zeigen aber, dass insbesondere CBC trotz der hypothetischen Abweichungen korrekte Nachfragekurven und Bepreisungsentscheidungen ermöglicht (Miller et al. 2011).

5 Latente Konstrukte

Zusätzlich zu den Ergebnissen der CBC werden demografische Informationen wie Alter, Familienstand, Einkommen und Geschlecht sowie psychografische Informationen erhoben. Die psychografischen Daten dienen als Basis für eine Cluster-Analyse (Green und Krieger 1991; Punj und Stewart 1983). Zur Messung der psychografischen Informationen werden erprobte Skalen aus IS, Marktforschung und Psychologie eingesetzt. Zur Messung des Vertrauens, das für Nutzerpräferenzen bezüglich IdMS bedeutend sein kann, wird das NEO Persönlichkeitsinventar (Costa und MacCrae 1992) verwendet. Für Sicherheitsaspekte könnte die Risikoaffinität entscheidend sein, weshalb auch diese anhand der relevanten Skala aus dem Jackson-Persönlichkeitsinventar (Jackson 1994) erhoben wird. Darüber hinaus werden verschiedene psychografische Eigenschaften ermittelt, deren generelle Auswirkung auf die Zahlungsbereitschaft belegt ist. Extravaganz (Cloninger et al. 1994) führt etwa typischerweise dazu, dass Konsumenten außergewöhnlich sein wollen, was sich in abweichendem Adoptionsverhalten niederschlägt. Generosität führt im Allgemeinen zu einer höheren WTP (Häusel 2001), während Preisbewusstsein diese senkt (Lichtenstein et al. 1993). Außerdem wurde der Grad der Meinungs-

führerschaft bestimmt (Childers 1986). Dies erlaubt es, die Einstellung starker Multiplikatoren zu IdMS zu bestimmen, die für die Diffusion entscheidend sein kann. Alle psychografischen Eigenschaften werden mit 7-Punkt-Likert-Skalen erhoben.

Die Eigenschaften dienen als Grundlage einer Marktsegmentierung auf Basis einer Cluster-Analyse, welche eine detailliertere Untersuchung der Präferenzen verschiedener Nutzergruppen bezüglich IdMS erlaubt.

6 Empirische Ergebnisse

Die Durchführung der Studie wurde Ende 2010 von einer führenden deutschen Marktforschungsfirma übernommen. Der Fragebogen war Web-basiert, die Befragung erfolgte pseudonym. Antworten wurden nur gewertet, wenn sie stichhaltig erschienen. Die Validität wurde über verschiedene Kriterien, etwa die zum Ausfüllen benötigte Zeit, ermittelt. Es wurde dabei kein irreguläres Verhalten beobachtet. Auf diese Weise eine Stichprobe zu erheben, ist kostspielig, hat aber einige Vorteile, beispielsweise eine Rücklaufquote von 100%.

6.1 Demografie

Es wurde eine repräsentative Stichprobe der erwachsenen deutschen Web-Population mit n=249 Antworten erhoben. Das durchschnittliche Alter betrug 41 Jahre (der Durchschnitt der deutschen Internetbevölkerung liegt nach Van Eimeren und Frees (2010) bei 40,65 Jahren) bei einer Standardabweichung von 11,5 Jahren, einem Minimum von 18 Jahren und einem Maximum von 64 Jahren. 141 Beantwortende (56,6%) sind männlich, 108 weiblich (43,4%). Dies spiegelt die in großangelegten Studien ermittelten Proportionen wieder (männlich: 54,3%, weiblich: 45,7%). Die durchschnittliche Anzahl von Personen pro Haushalt in der befragten Stichprobe ist 2,5. Die Mehrzahl der befragten Individuen sind verheiratet (45.8%) oder lebt in einer festen Partnerschaft (28,5%).

Ein Anteil von etwa 15% der Stichprobe besteht aus Studenten oder Praktikanten, die große Mehrheit (~55,4%) sind in einem Arbeitsverhältnis, 18,1% sind im Ruhestand oder arbeitslos. Auch dies ist für die deutsche Internetbevölkerung repräsentativ. Ungefähr 50% haben Abitur oder

auf andere Weise die Hochschulzugangsberechtigung erworben. 74 Befragte sind Absolventen einer Universität oder FH.

6.2 Psychografie

Cronbachs Alpha, eine Maßzahl für die interne Konsistenz der erhobenen psychografischen Faktoren, ähnelt den in den ursprünglichen Studien erhobenen Werten und liegt stets über der gängigen Schwelle von 0,7 (s. Tabelle 2). Die verwendeten Skalen sind also valide und zuverlässig.

Latentes Konstrukt	Cronbachs Alpha (diese Studie)	Cronbachs Alpha (Original)
Extravaganz	0,79	0,85
Preisbewusstsein	0,85	0,84
Meinungsführerschaft	0,95	0,79
Generosität	0,82	0,67
Risikobereitschaft	0,72	0,78
Vertrauen	0,80	0,82
Abenteuerlust	0,73	0,77

Tabelle 2: Cronbachs Alpha für latente Konstrukte

Darüber hinaus wurde eine explorative Faktoranalyse mit dem Varimax-Rotationsverfahren in SPSS durchgeführt. Diese identifizierte sieben Komponenten, welche die latenten Konstrukte widerspiegeln. Daraus folgt, dass die in der Umfrage erhobenen Daten die latenten Konstrukte beschreiben. Die Durchschnittswerte der latenten Konstrukte (s. Tabelle 3) werden als Grundlage für die weitere Analyse verwendet.

Latentes Konstrukt	Durchschnittswert
Extravaganz	5,5
Preisbewusstsein	2,9
Meinungsführerschaft	4,0
Generosität	3,6
Risikobereitschaft	5,3
Vertrauen	3,7
Abenteuerlust	3,5

Tabelle 3: Durchschnittswerte für latente Konstrukte

6.3 Resultate der Choice-Based-Conjoint-Analyse

Zur Ermittlung der Zahlungsbereitschaften wird HB mit *„standard diffuse priors"* genutzt. Die hier präsentierten Resultate wurden durch 20.000 analysierte Iterationen gewonnen, denen 40.000 verworfene Iterationen vorausgingen (insgesamt wurden also 60.000 Iterationen durchgeführt). Die Konvergenz wurde anhand von Wahrscheinlichkeits- und Parameterwerten abgeschätzt.

Die Validität der CBC wird durch die Bestimmung der internen Trefferquote (*internal hit rate*) und der mittleren absoluten Abweichung (*mean absolute deviation*, MAD) (Brazell et al. 2006) für die 14 Antwortmengen sowie der prädiktiven Trefferquote und mittleren absoluten Abweichung der zwei Testmengen ermittelt. Die Parameterabschätzungen werden genutzt, um die *first choice*-Trefferquote in den 16 Auswahlmengen und darüber die interne Validität zu bestimmen. Die *first choice*-Trefferquote misst die Frequenz, mit der die Analyse der CBC den gleichen ersten Rang vorhersagt, der beobachtet wird. Die zwei Testmengen wurden zur Feststellung der Vorhersagevalidität genutzt.

Die interne Trefferquote ist mit 93% exzellent, die interne MAD beträgt 10.74%. Die prädiktive Trefferquote beträgt sehr gute 88.2%, die prädiktive MAD ist 13.8%. Diese Werte liegen deutlich oberhalb des gängigen 1/3-Zufallskriteriums.

21 befragte Personen wählen niemals die Nicht-Kauf-Option, 139 befragte Personen wählen stets die Nicht-Kauf-Option. 55.8% der repräsentativen Stichprobe würden für ein Identitätsmanagement also nicht einmal 2 € im Jahr aufbringen, was die Opportunitätskosten der Teilnahme an einem solchen System nicht abdeckt. Diese Personen sehen also keinen Vorteil in der Teilnahme an einem IdM und bevorzugen Passwörter.

Befragte Personen, die stets oder niemals die Nicht-Kauf-Option wählen, werden nicht einbezogen, da ihre WTP nicht verlässlich geschätzt werden kann (siehe dazu Gensler et al. 2012).

6.4 Segmentierung

Innerhalb der befragten Stichprobe werden mittels einer einfach verketteten Clusteranalyse verschiedene Marktsegmente identifiziert. Diese werden anhand der erhobenen psychografischen Daten charakterisiert (s. Ta-

belle 4). Die Clusteranalyse liefert vier Segmente mit den folgenden Charakteristiken:

Kunden-segment	Extra-vaganz	Preis-bewusst-sein	Mei-nungs-führer-schaft	Genero-sität	Risiko-bereit-schaft	Vertrauen	Aben-teuerlust
1 (n=21)	5,31	3,00	3,01	3,16	3,55	3,98	2,48
2 (n=28)	5,64	2,11	4,50	4,15	5,86	4,20	4,10
3 (n=16)	4,41	1,92	2,01	2,90	5,64	2,85	3,06
4 (n=24)	5,73	4,13	4,38	3,13	5,14	3,46	3,85
Durchschnitt	5,37	2,83	3,68	3,42	5,08	3,71	3,46

Tabelle 4: Charakteristiken der Kundensegmente

Das erste Segment hat eine geringe Risikoaffinität und auch eine geringe Abenteuerlust. Daher werden diese Nutzer hier als “Risikoaverse” bezeichnet. Demografisch gibt es in diesem Segment mehr weibliche als männliche Nutzer, das Einkommen liegt über dem Durchschnitt. Das zweite Segment, das 28 prospektive Kunden aus der Stichprobe enthält (mehr männliche als weibliche), wird aufgrund seiner ausgeprägten Meinungsführerschaft als “Pioniere” bezeichnet. Diese Nutzer sind auch sehr risikoaffin und abenteuerlustig, typischerweise mit Pionieren assoziierte Eigenschaften. Das Einkommen ist unterdurchschnittlich. Segment 3 zeichnet sich durch eine geringe Meinungsführerschaft und Extravaganz aus. Nutzer in diesem Segment sind jedoch nicht sehr preisbewusst, was eine hohe WTP für Produkte anzeigen könnte, die sich bereits als nützlich für Pioniere erwiesen haben. Dieses Segment erhält daher die Bezeichnung “Folger”. Das letzte Segment erzielt in den meisten Skalen durchschnittliche Werte; dementsprechend erhält es den Bezeichner “Durchschnittliche Nutzer”. In den Segmenten 3 und 4 gibt es keine auffälligen demografischen Ausprägungen, was erneut die bessere Eignung der psychografischen Faktoren zur Segmentierung unterstreicht.

6.5 Bevorzugte Produkte und Zahlungsbereitschaft

Auf Basis der berechneten Nutzenwerte ist es möglich, die Zahlungsbereitschaften der Nutzer für Produkte mit verschiedenen Attributsausprägungen zu bestimmen. So lassen sich auch die optimalen Produkte für je-

des Segment ermitteln. Diese unterscheiden sich erheblich für die verschiedenen Segmente (s. Tabelle 5).

Kundensegment	Name	Bestes Produkt (a,b,c)* (WTP)	Zweitbestes Produkt (a,b,c)* (WTP)	Drittbestes Produkt (a,b,c)* (WTP)
1 (n=21)	Risikoaverse	3-1-2 47,80€	3-3-2 46,01€	3-2-2 43,83€
2 (n=28)	Pioniere	2-3-3 12,16€	3-3-3 10,95€	2-3-2 9,71€
3 (n=16)	Folger	2-1-3 35,95€	2-2-3 31,79€	2-1-2 29,86€
4 (n=24)	Durchschnittliche Nutzer	2-3-3 23,85€	2-1-3 23,42€	2-2-3 21,26€
Gesamt (n=89)	Alle Nutzer	2-1-3 18,10€	2-3-3 17,59€	2-2-3 16,30€
*Wobei (a, b, c) definiert wie folgt: a = 1 Identitätsattribute von Benutzer; a = 2 Zertifizierung der Identität; a = 3 Rechtsverbindliche Zusicherung; b = 1 IdP verwaltet Nutzerdaten; b = 2 Nutzer stellt Daten bereit; b = 3 Anonyme Credentials; c = 1 Nur nicht-kommerzielles Web; c = 2 Web inklusive E-Commerce; c = 3 E-Government, E-Commerce und private Kommunikation				

Tabelle 5: Zahlungsbereitschaften für präferierte IdMS-Gesamtprodukte

Mit maximal 48,70€ zeigen die Risikoaversen die höchste WTP. Diese Zielgruppe wünscht sich insbesondere ein rechtsverbindliches IdM für E-Commerce und nicht-kommerzielles Web. Der Privatsphärenschutz spielt für dieses Segment die geringste Rolle, es gibt aber eine Präferenz für die Verwaltung der Daten durch eine dritte Partei.

Demgegenüber haben die Pioniere insgesamt nur eine Zahlungsbereitschaft von 12,16€ pro Jahr für das von ihnen präferierte Produkt. Das Segment legt großen Wert auf die Möglichkeit, anonym aufzutreten. Das Segment zieht außerdem die breitestmögliche Anwendbarkeit vor, inklusive der Anwendung im E-Government, anders als das Segment der Risikoaversen. Um dieses Segment anzusprechen, müssten Anbieter anonymes Identitätsmanagement also für circa 10€ im Jahr anbieten, was etwa im Zuge einer zeitweisen Subventionierung zur Marktpenetration oder im Rahmen einer Gegenfinanzierung durch Einsparungen im E-Government-Bereich möglich wäre. Aufgrund der hohen externen Wertanteile könnten die Preise möglicherweise später angehoben werden.

Dies scheint insbesondere naheliegend, da das Segment der Folger eine erhebliche maximale WTP von 35,95€ hat. Die Folger lehnen anonyme

Credentials ab und präferieren zertifizierte Identifikation sowie einen möglichst breiten Anwendungsbereich.

Für die durchschnittlichen Nutzer wird eine maximale WTP von 23,85€ festgestellt. Auch diese Gruppe bevorzugt eine zertifizierte Identifikation und eine breite Anwendbarkeit. Im Gegensatz zu Folgern lehnen durchschnittliche Nutzer anonyme Credentials nicht ab, der Privatsphärenschutz ist ihnen jedoch relativ gleichgültig. Hier finden sich alle Ausprägungen unter den drei besten Systemen.

Da eine Produktdifferenzierung aufgrund der starken Netzwerkeffekte (Mueller et al. 2006) im Identitätsmanagement möglicherweise nicht wünschenswert ist, wird hier auch die Präferenz der Stichprobe als Ganzes analysiert. Die maximale WTP beträgt 18,10€, präferierte Ausprägungen sind zertifizierte Identifikation und breite Anwendbarkeit. Datenschutz spielt demgegenüber eine untergeordnete Rolle, auch die gesamte Stichprobe lehnt Datenschutzfunktionen sogar ab und hat die höchste WTP für die Verwaltung der Identität durch Dritte. Die insgesamt präferierte Ausprägung von IdM ist also eine dritte Partei, die Identitäten zertifiziert (allerdings nicht rechtsverbindlich) und die so breit wie möglich anwendbar ist.

7 Abgleich mit Marktsituation

In diesem Abschnitt wird die Relevanz der empirischen Ergebnisse zusätzlich überprüft, indem sie mit der tatsächlichen Entwicklung im Markt verglichen werden. Hierfür werden U-Prove, OpenID und Facebook betrachtet. Diese Systeme repräsentieren unterschiedliche technische Ansätze und sind gleichzeitig relevante IdMS für den Web-IdMS-Markt (Hühnlein et al. 2010; Maler und Reed 2008).

7.1 U-Prove

Die empirischen Resultate zeigen, dass die Nutzer Systeme mit starkem Privatsphärenschutz und rechtsverbindlicher Zertifizierung tendenziell eher ablehnen. U-Prove-Technologie wurde als CardSpace in das.NET-Framework 3.5 integriert und mit Windows Vista und Windows 7 ausgeliefert, hatte aber trotz dieser Nutzung der Verbreitung des Microsoft-Betriebssystems keinen Erfolg bei Nutzern oder Dienstanbietern. Aufgrund

unsere empirischen Ergebnisse ist dies nachvollziehbar: Eine Lösung mit anonymen Credentials würde höheres Vertrauen benötigen, eine Zielgruppe mit niedrigerer WTP ansprechen und höhere Kosten verursachen, die durch die geringe relative WTP kaum zu decken wären (Roßnagel 2006). Die Strategie von Microsoft, mit der Integration von MS Account seit Windows 8 eher auf eine auf Intermediation basierende Technologie zu setzen, ist also nachvollziehbar.

7.2 OpenID

Auch der vergleichsweise große Erfolg von OpenID lässt sich mit den empirischen Resultaten erklären: Die erfolgreichsten Implementierungen von OpenID nach (Landau und Moore 2011) entsprechen üblicherweise der Ausprägung mit der höchsten WTP für die gesamte Stichprobe. Besonders vielversprechend für den deutschen Markt scheint der Ansatz, zertifizierende OpenID-Anbieter einzurichten, die für bestimmte Anwendungsfälle und Kundengruppen sogar Rechtsverbindlichkeit anbieten können.

7.3 Facebook

Als dritte Partei spricht Facebook, ähnlich wie OpenID, sowohl in der Breite die meisten Nutzer an als auch die Nutzer mit den höchsten WTP für IdM. Facebook for Web Sites ist zwar im allgemeinen nicht für E-Commerce-Funktionen verwendbar, bietet aber Funktionen, die dort nützlich sind und unterstützt insgesamt die größte Anzahl von Diensten (Landau und Moore 2011). Zwar bietet Facebook keine Zertifizierung an, aber auch hier könnte man argumentieren, dass die Daten über Nutzer und ihre Beziehungen, die Facebook übermittelt, einem ähnlichen Zweck dienen. Facebook-Identitäten könnten dementsprechend, etwa im Rahmen der NSTIC-Initiative (Grant 2011) zertifiziert werden oder als Basis einer Zertifizierung dienen. In Kombination mit dem nicht direkt mit IdM verbundenen Nutzen, den Facebook seinen Nutzern stiftet, ist der Markterfolg dieser Plattform also wenig überraschend und deckt sich mit unseren empirischen Ergebnissen. Facebook illustriert sehr deutlich, dass Strategien, die IdM nicht als primäres Produkt, sondern als Nebeneffekt anderer, als nützlich empfundener Dienste vermarkten, sehr erfolgreich sein können.

8 Zusammenfassung

Prinzipiell scheint ein Markt für föderierte Identitätsmanagementsysteme vorhanden zu sein, da alle Marktsegmente eine substanzielle Zahlungsbereitschaft aufweisen. Da die Marktpioniere eine eher geringere WTP haben, bietet sich eine Penetrationspreisstrategie an, wobei der Preis später angehoben werden kann, sobald andere Kundensegmente einsteigen.

Weiterhin zeigt sich, dass Nutzer mit einer hohen Risikobereitschaft und einem hohen Maß an Vertrauensseligkeit nicht am Markt teilnehmen. Diese Teilnehmer konnten daher auch bei der Clusteranalyse nicht mehr berücksichtigt werden.

Unsere Ergebnisse deuten an, dass Privatsphärenschutz nur eine geringe Rolle für die Zahlungsbereitschaft spielt. Obwohl viele design-orientierte Forschungsarbeiten in der Vergangenheit angenommen haben, dass ein Bedarf für sicherere Systeme besteht, die immer höhere Sicherheits- und Privatsphärenschutz-Levels bieten, legen unsere Ergebnisse nahe, dass diese Eigenschaften bei weitem nicht so nachgefragt werden wie vermutet. Stattdessen kommen wir zu dem Resultat, dass Nutzer Systeme präferieren, bei denen ein Intermediär die Verwaltung der Nutzerdaten übernimmt. Dies ist auch am Markterfolg aktueller föderierter Identitätsmanagementsysteme zu erkennen, wo privatsphärenunfreundliche Systeme wie das von Facebook den Markt dominieren.

Die Schlussfolgerung liegt nahe, dass indirekte Netzwerkeffekte der führende Adoptionstreiber in diesem mehrseitigen Markt sind. Anbieter von FIM sollten sich daher mehr mit dem Henne-Ei-Problem befassen und geeignete Strategien entwickeln, um die Verbreitung ihrer Systeme voran zu treiben. Daher erscheint es auch zielführend, sich darauf zu konzentrieren, den wahrgenommenen Wert für die Nutzer zu erhöhen, anstatt immer neuere und kompliziertere Sicherheits- und Privatsphärenschutztechniken zu entwickeln.

Literatur

Acquisti, Alessandro (2008): "Identity Management, Privacy and Price Discrimination", in: *IEEE Security & Privacy* 6(2), 46-50.

Auty, Susan (1995): "Using Conjoint Analysis in Industrial Marketing: The Role of Judgement", in: *Industrial Marketing Management* 24(3), 191-206.

Backhouse James, Hsu Carol and *McDonnell Aiden* (2003): "Toward Public-Key Infrastructure Interoperability: Lessons from an Information Security Standard Accreditation Scheme", in: *Communications of the ACM (CACM)* 46(6), 98-100.

Bhatti Rafae, Bertino Elisa and *Ghafoor Arif* (2007): "An Integrated Approach to Federated Identity and Privilege Management in Open Systems", in: *Communications of the ACM (CACM)* 50(2), 81-87.

Brazell Jeff D., Diener Christopher G., Karniouchina Ekaterina v., Moore William L., Séverin Válerie and *Uldry Pierre-Francois* (2006): "The No-Choice Option and Dual Response Choice Designs", in: *Marketing Letters* 17(4), 255-268.

Camenisch, Jan and *Van Herreweghen, Els* (2002): "Design and Implementation of the idemix Anonymous Credential System", in: Atluri Vijayalakshmi (Ed.), *Proceedings of the 9th ACM Conference on Computer and Communications Security (ACM CCS'02),* ACM, 21-30.

Chapman Christopher N., Love Edwin and *Alford James L.* (2008): "Quantitative Early-Phase User Research Methods: Hard Data for Initial Product Design", in: Sprague, Ralph H. (Ed.), *Proceedings of the 41st Hawaii International Conference on System Sciences in Waikoloa, HI,* IEEE Computer Society, 37.

Childers, Terry L. (1986): "Assessment of the Psychometric Properties of an Opinion Leadership scale", in: *Journal of Marketing Research* 23, 184-188.

Cloninger, Claude R. (1994): *The Temperament and Character Inventory (TCI): A Guide to its Development and Use. Center for Psychobiology of Personality*, St. Louis, MO: Washington University Press.

Costa, Paul T. and *McCrae, Robert R.* (1992): *Revised NEO Personality Inventory (NEO-PI-R) and NEO Five-Factor Inventory (NEO-FFI) Professional Manual*, Odessa, FL: Psychological Assessment Resources.

Cummings, Ronald G. and *Taylor, Laura O.* (1999): "Unbiased Value Estimates for Environmental Goods: A Cheap Talk Design for the Contingent Valuation Method", in: *American Economic Review* 89(3), 649-665.

Dhamija, Rachna and *Dusseault, Lisa* (2008): "The Seven Flaws of Identity Management: Usability and Security Challenges", in: *IEEE Security & Privacy* 6(2), 24-29.

Evans, David (2003): "Some Empirical Aspects of Multi-Sided Platform Industries", in: *Review of Network Economics* 2(3), 191-209.

Fu Kevin, Sit Emil, Smith Kendra and *Feamster Nick* (2001): "Dos and Don'ts of Client Authentication on the Web", in: Wallach Dan S. (Ed.), *Proceedings of the 10th conference on USENIX Security Symposium (SSYM'01) in Washington D.C.*

Gelman Andrew, Carlin John B. and *Hal Stern S.* (2004): *Bayesian Data Analysis*, Boca Raton: Chapman & Hall/CRC.

Gensler Sonja, Hinz Oliver, Skiera Bernd and *Theysohn Sven* (2012): "Willingness-to-Pay Estimation with Choice-Based Conjoint Analysis: Addressing Extreme Response Behavior with Individually Adapted Designs", in: *European Journal of Operational Research,* 219(2), 368-378.

Grant, Jeremy A. (2011): "The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards", in: *Internet Computing* 15(6), 80-84.

Green, Paul E. and *Krieger, Abba M.* (1991): "Segmenting Markets with Conjoint Analysis", in: *The Journal of Marketing* 55(4), 20-31.

Haeusel, Hans-Georg (2000): *Der Umgang mit Geld und Gut in seiner Beziehung zum Alter*, Dissertation, TU München, http://mediatum.ub.tum.de/doc/603174/document.pdf.

Hansen Marit, Berlich Peter, Camenisch Jan, Clauß Sebastian, Pfitzmann Andreas and *Waidner Michael* (2004): "Privacy Enhancing Identity Management", in: *Information Security Technical Report* 9(1), 35-44.

Hühnlein Detlef, Roßnagel Heiko and *Zibuschka Jan* (2010): "Diffusion of Federated Identity Management", in: Freiling, Felix C. (Hrsg.), *Sicherheit 2010*, Bonn: Bonner Köllen Verlag, 25-36.

Ives Black, Walsh Kenneth R. and *Schneider Helmut* (2004): "The Domino Effect of Password Reuse", in: *Communications of the ACM (CACM)* 47(4), 75-78.

Jackson, Douglas N. (1994): *Jackson Personality Inventory: Revised Manual*, Port Huron: Research Psychologists Press.

Jøsang Audun, Zomai Muhammed al and *Suriadi Suriadi* (2007): "Usability and Privacy in Identity Management Architectures", in: Brankovic Ljiljana, Coddington Paul D., Roddick John, Steketee Chris, Warren James R. and Wendelborn Andrew L. (Eds.), *Proceedings of the fifth Australasian Symposium on ACSW Frontiers in Ballarat, Australia*, Australian Computer Society (ACS), 143-152.

Kormann, David and *Rubin, Aviel* (2000): "Risks of the Passport Single Signon Protocol", in: *Computer Networks* 33, 51-58.

Krolo Jacov, Silic Marin and *Srbljic Sinisa* (2009): "Security of Web Level User Identity Management", in: *Proceedings of the Information Systems Security*, *Croatian Society for Information and Communication Technology, Electronics and Microelectronics (MIPRO'09)*, 93-98.

Landau, Susan and *Moore, Tyler* (2011): "Economic Tussles in Federated Identity Management", in: Moore, Tyler and Friedman, Allan (Eds.), *The Tenth Workshop on Economics of Information Security (WEIS'11) in Fairfax, VA.*

Lichtenstein Donald R., Ridgway Nancy M. and *Netemeyer Richard G.* (1993): "Price Perceptions and Consumer Shopping Behavior: A Field Study", in: *Journal of Marketing Research* 30(2), 234-245.

Maler Eve and *Reed Daniel* (2008): "The Venn of Identity: Options and Issues in Federated Identity Management", in: *IEEE Security & Privacy* 6(2), 16-23.

Mannan Mohammad and *Van Oorschot Paul C.* (2007): "Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer", in: Dietrich, Sven and Dhamija, Rachna (Eds.), *Proceedings of the 11th international Conference on Financial Cryptography and 1st international Conference on Usable Security*, *Scarborough, Trinidad and Tobago*, 88-103.

Miller Klaus M., Hofstetter Reto, Krohmer Harley and *Zhang John* (2011): "How Should We Measure Consumers' Willingness to Pay? An Empirical Comparison of State-of-the-Art Approaches", in: *Journal of Marketing Research* 48(1), 172-184.

Moorthy Sridha, Ratchford Brian T. and *Talukdar Debabrata* (1997): "Consumer Information Search Revisited: Theory and Empirical Analysis", in: *Journal of Consumer Research* 23(4), 263-277.

Mueller Milton L., Park Yuri, Lee Jongsu and *Kim Tay-yoo* (2006): "Digital Identity: How Users value the Attributes of Online Identifiers", in: *Information Economics and Policy* 18(4), 405-422.

Neumann, Peter G. (1994): "Risks of Passwords", in: *Communications of the ACM (CACM)* 37(4), 126.

Punj, Girish and *Stewart, David W.* (1983): "Cluster Analysis in Marketing Research: Review and Suggestions for Application", in: *Journal of Marketing Research* 20(2), 134-148.

Recordon, David and *Reed, Drummond* (2006): "OpenID 2.0: A Platform for User-centric Identity Management", in: Juels Ari, Winslett Marianne and Atsuhiro Goto (Eds.), *Proceedings of the second ACM Workshop on Digital Identity Management (DIM'06)*, *Alexandria, VA*, ACM Press, 11-16.

Roßnagel, Heiko (2006): "On Diffusion and Confusion – Why Electronic Signatures Have Failed", in: Fischer-Hübner Simone, Furnell Steven and Lambrinoudakis Costas (Eds.), *Trust and Privacy in Digital Business*, Berlin and Heidelberg: Springer, 71-80.

Roßnagel Heiko, Zibuschka Jan, Hintz Oliver and Muntermann Jan (2014): "Users' willingness to pay for web identity management systems", in: *European Journal of Information Systems*, 23(1), 36–50.

Schläger Christian, Sojer Manuel, Muschall Björn and *Pernul Günther* (2006): "Attribute-Based Authentication and Authorisation Infrastructures for E-Commerce Providers", in: Bauknecht Kurt, Pröll Birgit and Werthner Hannes (Eds.), *E-Commerce and Web Technologies*, Berlin and Heidelberg: Springer, 132-141.

Street, Deborah J. and *Burgess, Leonie* (2007): "The Construction of Optimal Stated Choice Experiments", in *Theory and Methods. Wiley-Interscience*, New Jersey: John Wiley & Sons Inc.

Van Eimeren, Birgit und *Frees, Beate* (2010): „Fast 50 Millionen Deutsche online – Multimedia für alle", in *Media Perspektiven* 7-8, 334-349.

Zibuschka, Jan (2014): *Ein Vorgehensmodell zum Entwurf tragfähiger Sicherheitsinfrastrukturen*, Stuttgart: Fraunhofer Verlag.

Zibuschka, Jan and *Roßnagel, Heiko* (2008): "Implementing Strong Authentication Infrastructure Interoperability with Legacy Systems", in: de Leeuw Elisabeth, Fischer-Hübner Simone, Tseng Jimmy C. and Borking John (Eds.), *Policies and Research in Identity Management*, Boston: Springer, 149-160.

Zibuschka, Jan and *Roßnagel, Heiko* (2012): "On some conjectures in IT-security: The case for viable security solutions", in: Suri, Neeraj and Waidner, Michael (Eds.), *Sicherheit 2012: GI-Edition – Lecture Notes in Informatics (LNI), P-195,* Bonn: Bonner Köllen Verlag, 25-33.

Autorenverzeichnis

Jens Bender, Dr. rer. nat., Mathematiker, ist Referatsleiter im Bundesamt für Sicherheit in der Informationstechnik (BSI) im Referat „eID-Technologien und Chipkarten“. Er befasst sich mit Themen rund um elektronische Identifizierung, hoheitliche Dokumente und Public-Key-Infrastrukturen.

Tile von Damm, Dipl. Pol. ist Leiter von MOD-Institute (www.mod.org.in) und Mitglied der DIN/ISO-Working Group Smart City. Er forscht zu globalen Governance-Strukturen, Partizipation und Teilhabe, städtischer Integration, nachhaltiger urbaner Entwicklung, Smart Cities, Forschungspolitik und -transfer und dezentralen Infrastrukturen.

Johannes Eichenhofer, Dr. jur, ist PostDoc an der Fakultät für Rechtwissenschaft der Universität Bielefeld. Forschungen zum Migrations- und Integrationsrecht, zum deutschen und europäischen Grundrechtsschutz, zum Privatheitsschutz und zum Sicherheitsrecht.

Christoph Engemann, Dr. des., ist Post-Doc an der DFG-Kollegforschergruppe Medienkulturen der Computersimulation der Leuphana Universität Lüneburg. Forschung zur Geschichte von Authentifikationsmedien, elektronischen Gesundheitskarte, Gouvernemedialität, sowie zu Social-Graphs und ihrer Geschichte.

Hannes Federrath, Dr.-Ing., ist seit 2011 als Universitätsprofessor am Fachbereich Informatik der Universität Hamburg Leiter des Arbeitsbereichs Sicherheit in verteilten Systemen. Arbeitsschwerpunkte: Sicherheit und Schutz im Internet, IT-Sicherheits- und Risikomanagement, Kryptographie, Mobile Computing und technischer Datenschutz.

Christoph Gusy, Dr. jur., ist Universitätsprofessor für Öffentliches Recht, Staatslehre und Verfassungsgeschichte an der Fakultät für Rechtswissenschaften der Universität Bielefeld. Forschungen zu Neuerer und Neuester Verfassungsgeschichte, Grundrechtsfragen, Sicherheitsrecht, Informations- und Datenschutzrecht.

Dominik Herrmann, Dr. rer nat., ist Post-Doc am Arbeitsbereich Sicherheit in verteilten Systemen an der Universität Hamburg. Forschung zu Angriffen auf

die Privatsphäre, Tracking von Internetnutzern sowie zur Gebrauchstauglichkeit von Datenschutz-Techniken und -Prozessen.

Oliver Hinz, Dr. rer. pol., ist Leiter des Fachgebiets Wirtschaftsinformatik | Electronic Markets an der Technischen Universität Darmstadt. Seine Forschung ist an der Schnittstelle von Märkten und Technologien angesiedelt.

Gerrit Hornung, Dr. jur., ist Universitätsprofessor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel. Forschung zu den verfassungsrechtlichen Grundlagen des IT-Rechts, E-Government, IT-gestützte Geschäftsprozesse, Datenschutz- und IT-Sicherheitsrecht sowie zur rechtswissenschaftlichen Innovationstheorie.

Lexi Pimenidis, Dr. rer. nat., arbeitet als freiberuflicher Berater zu den Themen Sicherheit, Datenschutz und elektronische Bezahlsysteme. Neben der Arbeit hält er Vorträge und Schulungen an Universitäten sowie als Einführungsveranstaltungen für die Allgemeinheit.

Jan Muntermann, Dr. rer. pol., ist Inhaber der Professur für Electronic Finance und Digitale Märkte an der Georg-August-Universität Göttingen. Seine Forschung widmet sich den digitalen Transformationen von Unternehmen und Märkten.

Jan Schallaböck, Dr. des., ist Partner bei iRights.Law Rechtsanwälte in Berlin. Vor seiner anwaltlichen Tätigkeit arbeitete und forschte er als Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein in verschiedenen Projekten zu „Datenschutztechnologien und Identitätsmanagement“. Seit 2007 begleitet er auch die gleichnamige Arbeitsgruppe in ISO/IEC, deren stellvertretender Vorsitzender er ist.

Heiko Roßnagel, Dr. rer. pol., leitet das Competence Team Identitätsmanagement am Fraunhofer Institut für Arbeitswirtschaft und Organisation. Seine Forschung beschäftigt sich mit wirtschaftlicher und nutzerfreundlicher Gestaltung und Verwendung von Sicherheitslösungen.

Jan Zibuschka, Dr.-Ing., ist in der zentralen Forschungsabteilung der Robert Bosch GmbH im Bereich Sicherheit, Datenschutz und Informationssysteme tätig. Insbesondere gilt sein Interesse dem nutzerzentrischen Entwurf von Sicherheits- und Datenschutzinfrastrukturen, vor allem in den Bereichen Transparenz, Intervenierbarkeit und Identitätsmanagement.