Digitale Identitäten in Deutschland:

Ergebnispapiere von acht Workshops im Zeitraum Mai 2018 - Januar 2020

Verimi-Begleitforschungsprojekt des Digital Society Institute, ESMT Berlin

Martin Schallbruch, Tanja Strüve und Isabel Skierka

Mai 2020

Übersicht

Vom 1. Januar 2018 bis zum 31. März 2020 hat das Digital Society Institute (DSI) der ESMT Berlin ein Begleitforschungsprojekt zu digitalen Identitäten mit Unterstützung der Verimi GmbH durchgeführt. Im Rahmen des Projekts fanden acht halbtägige Fachworkshops mit jeweils 15 bis 30 externen Experten und Praktikern unterschiedlicher Stakeholdergruppen aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft sowie eine Konferenz zu digitalen Identitäten an der ESMT Berlin statt. Die Workshops befassten sich mit der Rolle digitaler Plattformen im Bereich des digitalen Identitäten-Managements in spezifischen Sektoren sowie mit sektorübergreifenden Fragestellungen hinsichtlich der Daseinsvorsorge, Datenschutz und -souveränität sowie Interoperabilität, Offenheit und Datenportabilität. Die Ergebnisse der Fach-Workshops sind in den folgenden acht Papieren zusammengefasst.

Inhaltsverzeichnis

1. Ergebnispapier zur *Plattformdebatte Gesundheit* (Mai 2018) *2*
2. Ergebnispapier zur *Plattformdebatte Daseinsvorsorge und Kritische Infrastruktur* (Juni 2018) *6*
3. Ergebnispapier zur *Plattformdebatte Mobilität 4.0* (Juli 2018) *11*
4. Ergebnispapier zur *Plattformdebatte Interoperabilität, Offenheit und Datenportabilität* (August 2018) *15*
5. Ergebnispapier zur *Plattformdebatte Datenschutz und Datensouveränität* (September 2018) *20*
6. Ergebnispapier zur *Plattformdebatte Digitale Bildung* (November 2018) *24*
7. Ergebnispapier zur *Plattformdebatte Smart Home* (Januar 2019) *29*
8. Ergebnispapier zur *Debatte Digitale Identitäten im Gesundheitswesen* (Januar 2020) *35*
9. Fazit *41*

Plattformdebatte Gesundheit – Mai 2018

Martin Schallbruch, Tanja Strüve und Isabel Skierka

Im Mai 2018 war das Digital Society Institute Gastgeber der Plattformdebatte Gesundheit, die im Rahmen eines Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen für die Verimi GmbH ausgerichtet wurde. Die Veranstaltung befasste sich mit der Digitalisierung im Gesundheitswesen und mit der Frage, welche Rolle digitale Plattformen dabei einnehmen können. Impulsvorträge trugen Florian Bontrup (Docyet UG), Ingo Horak (Uvita GmbH), Ralf Degner (TK) und Miriam van Straelen (Verimi GmbH) zu der Debatte bei.

1. Sachstand

Die zunehmende Digitalisierung nahezu aller Lebensbereiche verändert auch das deutsche Gesundheitswesen. Insbesondere bei der medizinischen Versorgung strukturschwacher Regionen, den Herausforderungen des demografischen Wandels und den Finanzierungslücken aufgrund steigender Gesundheitsausgaben eröffnet die Digitalisierung neue Möglichkeiten für Kosteneinsparungen und den leichteren Zugang zu Gesundheitsangeboten.

Die Entwicklungen sind geprägt von einem Spannungsverhältnis zwischen dem Bedürfnis der Patienten nach innovativen digitalen Angeboten einerseits und der besonderen Sensitivität von Gesundheitsdaten und der damit verbundenen Regulierungsintensität und Schutzbedürftigkeit der Daten andererseits. Die Risiken im Hinblick auf die Nutzung digitaler Technologien im Gesundheitssektor beziehen sich insbesondere auf etwaige Mängel beim Datenschutz oder der IT-Sicherheit.

Die ersten Grundlagen für digitale Anwendungen im Bereich des Gesundheitswesens wurden bereits durch das 2003 verabschiedete *Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz)* geschaffen, aufgrund dessen digitale Anwendungen im SGB V implementiert wurden. Gemäß § 291a Abs. 1 SGB V wurden digitale Anwendungen für die elektronische Gesundheitskarte (eGK) festgelegt. 2015 wurden durch das *Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen*, dem sogenannten *eHealth-Gesetz* konkrete Anwendungen und Zeitpläne für die Einführung einer digitalen Infrastruktur festgelegt. Ziel des Gesetzes ist es u.a., den Rollout ausgewählter Anwendungen sowie die flächendeckende Interoperabilität herzustellen. Dabei soll die Telematikinfrastruktur (TI) die Voraussetzungen für den Austausch von Gesundheitsdaten schaffen.

Im staatlich finanzierten Teil des Gesundheitsmarktes (im sogenannten ersten Gesundheitsmarkt) ist die Nutzung digitaler Angebote bislang eingeschränkt. Auf dem zweiten Gesundheitsmarkt, welcher alle privat finanzierten Produkte und Dienstleistungen rund um die Gesundheit umfasst, werden zunehmend eHealth-Anwendungen in Anspruch genommen, wie beispielsweise Apps

für Smartphones, Telekonsil und „Wearables“. Diese Situation spiegelt auch den allgemeinen Trend der weit verbreiteten Nutzung digitaler Angebote wider.[1] Krankenkassen wie die AOK und die Techniker Krankenkassen (TK) bieten ihren Versicherten dementsprechend zunehmend digitale Anwendungen an. Die TK hat in Zusammenarbeit mit IBM eine elektronische Patientenakte entwickelt, die es den Versicherten ermöglicht, mittels einer App auf ihre gespeicherten Gesundheitsdaten zuzugreifen.

Aufgrund hoher Eintrittsbarrieren ist der Marktzugang für innovative Anbieter in den ersten Gesundheitsmarkt schwierig. Der Zugang zur Regelversorgung ist grundsätzlich langwierig, teuer, komplex und wenig transparent.[2] Zudem ist eine Interoperabilität der informationstechnischen Systeme derzeit nicht gegeben. Zusätzlich erschwert das Fehlen einheitlicher Rahmenbedingungen und verbindlicher Standards den Zugang zum ersten Gesundheitsmarkt.[3]

Eine zentrale Frage ist, welche Rolle digitalen Plattformen in diesem Kontext zukommen kann. In einer vernetzten digitalen Welt nimmt die Bedeutung digitaler Plattformen stetig zu. Sie fungieren als digitaler Marktplatz und bieten für Unternehmen Erleichterungen dabei, neue Geschäftsmodelle aufzubauen und Kosten für Nicht-Kernfunktionen einzusparen. Digitale Plattformen bringen damit als zentrale Knotenpunkte Anbieter und Nachfrager auf dem Markt zusammen. Sofern Plattformen hohe Sicherheitsstandards garantieren, können sie den Nutzer digitaler Angebote dabei unterstützen, die Souveränität über die eigenen Daten zu wahren.

Auch die Bundesregierung hat sich im Koalitionsvertrag zu einer Stärkung nationaler und europäischer Plattformen bekannt, sie will insbesondere ein *Level playing field* herstellen und Portabilität schaffen.

2. Anforderungen an Plattformen im Gesundheitswesen

Im Gesundheitswesen könnten Plattformen dazu genutzt werden, Angebote von Gesundheitsdienstleistern und den Nachfragern, insbesondere den Patienten zu koordinieren. Darüber hinaus ermöglichen sie die Integration unterschiedlicher Dienste wie beispielsweise Telemedizin und die Einbeziehung verschiedener Datenquellen wie die elektronischer Patientenakte, „Wearables“ und andere. Plattformen, die im Gesundheitswesen eingesetzt werden sollen, sollten folgende Anforderungen erfüllen.

Patientenzentrierung

Einigkeit bestand unter den Workshop-Teilnehmern darüber, dass digitale Plattformen im Gesundheitsbereich auf die Bedürfnisse der Endanwender und damit insbesondere der Patienten ausgerichtet sein müssen. Viel genutzte digitale Gesundheitsangebote in Form von Apps und Wearables haben gemeinsam, dass sie niederschwellig, leicht und einfach bedienbar sind. Darüber hinaus ist die Bereitschaft zur Nutzung dann gegeben, wenn die Anbieter den Nutzern aus einem anderen Kontext bekannt und bewährt sind. Dies ist beispielsweise bei der von Apple bereitge-

[1] Das Statistikportal (2018). https://de.statista.com/statistik/daten/studie/13070/umfrage/entwicklung-der-internet-nutzung-in-deutschland-seit-2001/
[2] Bundesministerium für Wirtschaft und Energie (2017). Digitalisierung der Gesundheitswirtschaft. Eckpunktepapier.
[3] Strategy & und pwc (2016). Weiterentwicklung der eHealth-Strategie - Studie im Auftrag des Bundesministeriums für Gesundheit. https://www.bundesgesundheitsministerium.de/ministerium/meldungen/2016/big-data-anwendungen/?L=0

stellten Gesundheitsakte der Fall. Die App ist ansprechend und übersichtlich gestaltet und bietet Möglichkeiten zur praktischen Verwaltung von Gesundheitsdaten der Nutzer. Darüber hinaus kann sich die Nutzerin einfach und direkt mit ihrer Apple-Identität authentifizieren. Datenschutzrechtliche oder andere Bedenken stehen dabei für viele Nutzer im Hintergrund.

Eine erfolgreiche Plattform im Gesundheitswesen sollte also die Bedürfnisse der Patienten in den Vordergrund stellen und ohne große Hindernisse einfach nutzbar sein. In diesem Sinne sollte sich die Patientin auch leicht authentifizieren und ihre Daten einfach und übersichtlich verwalten können. Die Möglichkeit zur differenzierten Verwaltung von Daten, einschließlich von deren Privatsphäre und Weitergabe, erlaubt es der Patientin, Souverän ihrer Daten zu sein.

Die Teilnehmer waren sich ebenfalls einig darüber, dass der erste Gesundheitsmarkt, und damit der Regelversorgungsbereich, zu komplex für viele Patienten und die Patientenzentriertheit der Angebote nicht ausreichend ist.

Datenschutz und Datensicherheit

Sofern eine Plattform Gesundheitsleistungen in ihr Geschäftsmodell integrieren will, muss sie aufgrund der besonderen Sensibilität personenbezogener Gesundheitsdaten hohe Datenschutz- und Datensicherheitsstandards aufweisen.

In rechtlicher Hinsicht müssen Plattformen die datenschutzrechtlichen Vorgaben der DSGVO umsetzen und dabei auch die neuen Vorschriften des BDSG beachten.

Dieses gilt im Kontext medizinscher Dienstleistung in besonderem Maße, da es sich bei den Daten um Gesundheitsdaten handelt, die gemäß Art. 9 DSGVO einem besonderen Schutz unterliegen. Die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit müssen durch technische Maßnahmen sichergestellt werden. Dabei kommen insbesondere voll verschlüsselte Systeme in Betracht, wenngleich hier ein Spannungsfeld zu den Möglichkeiten erweiterter Datenanalysen besteht. Sie sind auf vollverschlüsselten Systemen nicht möglich.

Empfehlenswert ist zusätzlich eine datenschutzrechtliche Zertifizierung anzustreben, um ein hohes Datenschutzniveau der Plattform im medizinischen Kontext nachweisen zu können. Im Ergebnis müssen Plattformen also eine Balance zwischen Leistungsfähigkeit, Usability und Sicherheit gewährleisten.

Erhalt der Souveränität

Viele Akteuren sehen die Anwendungslandschaft der TI als zu starr für die sinnvollen digitalen Innovationen im Gesundheitswesen an. Jedoch forderten mehrere Workshop-Teilnehmer, dass Plattformen neue Anwendungen im Gesundheitsbereich dabei unterstützen müssen, eine Kontrollierbarkeit der Angebote, auch durch das öffentlich verantwortete Gesundheitswesen, zu erhalten. Dazu gehört auch die Sicherstellung der digitalen Souveränität des Patienten.

Offenheit

Eine Plattform im Gesundheitsbereich sollte offen zugänglich für alle beteiligten Akteure sein, also Anbieter von digitalen Gesundheitsangeboten sowie Leistungserbringern und Krankenkassen. Eine Plattform kann, wie oben angedeutet, Transaktionskosten reduzieren und Netzwerkeffekte unter allen Beteiligten erzielen – was allerdings derzeit, insbesondere im ersten Gesundheitsmarkt, aufgrund der hohen Eintrittsbarrieren erschwert ist.
Aus Sicht der Akteure des Gesundheitswesens ist die zentrale Herausforderung der nächsten Jahre, eine „Öffnungsstrategie“ zu erarbeiten, die es erlaubt, neue Anwendungen im Gesundheitsbereich einzusetzen und hierbei Daten mit den vorhandenen Systemen bei Leistungserbringern und Krankenversicherung sowie auch den Patienten auszutauschen.

Sicherstellung von Interoperabilität

Um eine breite Implementierung der Plattform im Gesundheitswesen zu erreichen, sind zusätzlich offene Schnittstellen erforderlich. Auf diese Weise könnte ein umfassender Zugang für alle Stakeholder des Gesundheitswesens, d.h. niedergelassene Ärzte, Krankenhäuser und Krankenkassen, gewährleistet werden. Nur über solche offenen Schnittstellen und einheitliche Standards kann eine nahtlose Kommunikation zwischen existierenden und geplanten Systemen, Anwendungen oder Komponenten hergestellt werden. Zusätzlich

sollten Plattformen im Gesundheitswesen - soweit möglich - mit der TI interoperabel sein. Aus dem eHealth-Gesetzes folgt, dass die TI für solche Anwendungen, die von der eGK unabhängig sind, in Zukunft geöffnet werden soll. Um eine solche Interoperabilität zu gewährleiste sieht das eHealth-Gesetz vor, dass die gematik ein Verzeichnis führen wird, in dem Standards veröffentlicht werden. Durch dieses soll die Kommunikation verschiedener IT-Systeme im Gesundheitswesen verbessert werden.

Die in diesem Verzeichnis aufgeführten Standard könnten ebenfalls hilfreich für Plattformen im Gesundheitsbereich sein.

Authentifizierung und Identifizierung

Eine Plattform im Gesundheitsbereich muss als technisch-organisatorische Maßnahme im Sinne des Art. 32 DSGVO eine adäquate Authentifizierung beinhalten, so dass sichergestellt ist, dass nur Berechtigte auf die besonders sensiblen Daten zugreifen können. Eine solche ist im Hinblick auf die Patienten aber auch auf die Leistungserbringer und Krankenkassen erforderlich. Im Bereich der Regelversorgung ist eine solche durch das eHealth-Gesetzes in § 291a Absatz 5 Satz 5 SGB V schon heute in vorgesehen, aus dem sich ergibt dass beispielsweise auf Daten der elektronischen Patientenakte nur mittels der eGK und des elektronischen Heilberufeausweises (2-Schlüsselprinzip) zugegriffen werden kann.

Im Bereich der Identifizierung von Patienten über Plattformen besteht noch Klärungsbedarf. Bisherige Verfahren sind papierbasiert. Es bestehen noch keine einheitlichen Standards zur digitalen Authentifizierung und Identifizierung. Eine elektronische Identifizierung über die Gesundheitskarte ist bisher nur für ausgewählte Anwendungen möglich. Zwar existieren verschiedene Identifizierungsverfahren wie Video-Ident u.a. Diese sind jedoch sehr kostenaufwändig und damit nicht im Gesundheitswesen skalierbar. Eine digitale Plattform könnte diese Skalierung ermöglichen.

Plattformdebatte Daseinsvorsorge und Kritische Infrastruktur – Juni 2018

Martin Schallbruch, Tanja Strüve und Isabel Skierka

Im Juni 2018 war das Digital Society Institute Gastgeber der Plattformdebatte Daseinsvorsorge und Kritische Infrastruktur, die im Rahmen eines Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen mit der Verimi GmbH ausgerichtet wurde. Die Veranstaltung ging der zentralen Frage nach, inwiefern und inwieweit digitale Plattformen als Teil der Daseinsvorsorge zu verstehen und in weiterer Folge als kritische Infrastruktur einzuordnen sind. Impulse zu der Debatte steuerten Frank-Rüdiger Srocke (Bundesministerium des Innern, für Bau und Heimat), Dr. Marianne Wulff (Dataport AöR) und Dr. Waldemar Grudzien (COREtransform GmbH) bei.

1. Sachstand

Digitale Plattformen und Daseinsvorsorge

Digitale Plattformen haben eine überragende Bedeutung in unserer digitalen Welt. Sie fungieren als zentrale Knotenpunkte im Netz, sie sind Interessenabgleicher, Datenverarbeiter, Innovationstreiber und Marktmacher. Ihre Rolle hat sowohl politische, gesellschaftliche, ökonomische sowie rechtliche Dimensionen. Bei genauerer Betrachtung digitaler Plattformen stellen sich Fragen des Datenschutzes der Nutzer, der IT-Sicherheit, der Datensouveränität, des Wettbewerbs sowie die Frage nach der Verantwortung für die abgebildeten Inhalte. Im Koalitionsvertrag haben die tragenden Parteien der Bundesregierung festgelegt, nationale und europäische Plattformen stärken zu wollen. Die Bedeutung digitaler Plattformen als Organisationsformen der digitalen Gesellschaft und Wirtschaft wird in Zukunft nur noch weiter steigen.

Angesichts dieser zentralen Rolle und Bedeutung der Plattformen stellt sich die Frage, ob sich für den Staat im Hinblick auf die Plattformen eine Daseinsvorsorgepflicht ergibt und inwiefern und inwieweit digitale Plattformen als kritische Infrastrukturen einzustufen sind. Unter dem Begriff Daseinsvorsorge wird die Bereitstellung notwendiger Güter und Leistungen verstanden, die für ein sinnvolles menschliches Dasein notwendig sind. Den Staat trifft die Pflicht, die Bedürfnisbefriedigung der Bürger zu garantieren und die sozio-kulturelle Teilhabe sicherzustellen.[4] Was im Einzelnen unter Daseinsvorsorge zu verstehen ist, hängt maßgeblich von vielfältigen Einflussfaktoren in Politik, Privatwirtschaft, dem Markt und gesellschaftlich bedeutenden Interessen ab und ist immer das Ergebnis einer politischen Entscheidung.

Auch klassische gesellschaftliche Funktionen, wie Zahlungsmittel oder Meinungsbildung, werden digital neu definiert und zu Infrastrukturen für digitale Geschäftsmodelle. In allen Bereichen werden Identifizierungssysteme benötigt, sowohl in

[4] (BVerfG, Beschluss vom 23. November 1988 – 2 BvR 1619/83 –, BVerfGE 79, 127-161, Rn. 40)

den einzelnen gesellschaftlichen Sektoren wie Gesundheit und Mobilität als auch bei Querschnittsfunktionen wie den oben genannten Finanztransaktionen, der Meinungsbildung, der Kommunikation oder Cloud-Angeboten zur Speicherung von Daten. Viele dieser Funktionen werden zunehmend von digitalen Plattformen übernommen, zum Beispiel von Facebook, Google oder PayPal. Mit ihrem Facebook- oder Google-Konto können sich Nutzer bei zahlreichen Diensten authentifizieren. Systeme zum Management digitaler Identitäten werden zu einem essenziellen Bestandteil der Nutzung digitaler Plattformen.

Insofern ist über Einordnung und Reichweite digitaler Plattformen als Teil der Daseinsvorsorge zu diskutieren. Sofern und soweit dies der Fall ist, schließt sich die Frage an, inwieweit sie darüber hinaus auch als Kritische Infrastruktur einzuordnen sind. Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Noch weitergehend als ohnehin im Bereich der Daseinsvorsorge trifft den Staat bei den Kritischen Infrastrukturen die Pflicht, ihre Funktionsfähigkeit sicherzustellen, um elementare Lebensbedürfnisse der Menschen zu gewährleisten.

Digitale Plattformen als Verwalter digitaler Identitäten

Aufgrund des herausragenden Stellenwerts digitaler Identitäten als Schlüssel und Klammer der Nutzung digitaler Angebote und Dienstleistungen konzentrierte sich die Debatte auf Plattformen, die digitale Identitätsmangement-Systeme anbieten.

Digitale Plattformen bieten ihren Nutzern typischerweise verschiedene Dienste an, um ihre Identität im digitalen Raum zu verwalten. Sie basieren in der Regel auf einer initial verifizierten Identität und umfassen Leistungen wie ein Single-Sign-On sowie Verwaltungs-, Auswertungs- und Sicherheitsfunktionen rund um die digitale Identität. Internationale Hyperplattformen nutzen elektronische Identitäten und zentrale Benutzerkonten überdies zur Markterschließung und tragen damit zu einer immer größeren Marktkonzentration bei.

Digitale Identitäten und deren Vulnerabilität

Die verlässliche Identifizierung einer Person durch Reisepässe als multifunktionale hoheitliche Identifizierungsdokumente spielte bereits im Mittelalter eine tragende Rolle.

Im digitalen Raum ohne territoriale Grenzen haben staatliche Identifizierungsinstrumente indes bislang keine große Verbreitung gefunden. Mit der zunehmenden Verlagerung der unterschiedlichen Lebensbereiche in den digitalen Raum steigt gleichwohl auch dort der Bedarf nach einer sicheren und verlässlichen Identifizierung. Dies gilt gleichermaßen für Nutzer digitaler Dienste sowie für Maschinen im Internet der Dinge. Wie entscheidend verifizierte digitale Identitäten sind, zeigt eine Studie von PricewaterhouseCoopers aus dem Jahre 2016. Danach gaben 33 Prozent der Internetnutzer an, bereits einmal von einem Identitätsdiebstahl betroffen gewesen zu sein.[5]

Einigkeit unter den Workshop-Teilnehmern bestand darüber, dass verlässlichen digitale Identitäten eine essenzielle Rolle in unserer Gesellschaft zukommt und ihre Bedeutung mit der steigenden Transformation analoger in digitale Abläufe in Zukunft deutlich steigen wird. Die virulente Frage nach Transparenz und Steuerung sowie die Rolle des Staates wird damit in Zukunft zu beantworten sein.

Staatliche Angebote für digitale Identitäten

Die Bundesregierung verfolgt das Ziel, die öffentliche Verwaltung flächendeckend zu digitalisieren.

Das 2017 verabschiedete Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (OZG) verpflichtet Bund und Länder, alle geeigneten Verwaltungsleistungen binnen 5 Jahren, bis 2022, auch online anzubieten und diese über den Portalverbund zugänglich zu machen. Der Portalverbund soll dazu dienen, die Verwaltungsportale

[5] PwC Studie 2016; Identitätsklau – die Gefahr aus dem Netz, S. 8, abrufbar unter https://www.pwc.de/de/handel-und-konsumguter/assets/cyber-security-identitaetsdiebstahl-2016.pdf

von Bund und Ländern zu verknüpfen, so dass Bürger und Unternehmen die Online-Leistungen leicht finden und über das für sie angelegte Nutzerkonto abwickeln können. Der Portalverbund soll Basisdienste in Form eines Nutzerkontos, eines Datensafes, eines Content-Management-Systems, eines Formular-Managements, einer E-Payment- sowie einer Suchfunktion bieten. Außerdem soll er an das Single Digital Gateway der EU angeschlossen werden und so – auch zur Unterstützung der Umsetzung des „Once Only"-Prinzips – die Integration europäischer Anforderungen gewährleisten.

Je nach Art der Verwaltungsleistungen sind die Anforderungen an eine sichere Identifizierung unterschiedlich. Im Hinblick auf das im Portalverbund erforderliche Identitätsmanagement wird sich die jeweils angemessene Identifizierung nach dem erforderlichen Vertrauensniveau der begehrten Verwaltungsleistung richten. Aus Sicht der Bürger soll eine einheitliche und einfache Identifizierung über das Nutzerkonto („Servicekonto") möglich werden. Erforderlich sind dafür die Erarbeitung von Vorgaben für die anzuwendenden Standards, Schnittstellen und Sicherheitskomponenten nach dem OZG und darüber hinaus die Prüfung, inwieweit auf vorhandene Lösungen zurückgegriffen werden kann. Eine Identifizierungs-Lösung im Portalverbund muss die aus der europäischen eIDAS-Verordnung folgende Verpflichtung der EU-Mitgliedsstaaten berücksichtigen, die eIDAS-Sicherheitsniveaus abzubilden und eIDAS-notifizierte Identitätsmanagementsysteme zuzulassen. Private Anbieter eines digitalen Identitätsmanagementssystems müssen im Hinblick darauf eine eIDAS-Notifizierung herbeiführen.

IT-Dienstleister wie Dataport agieren als Service Provider der öffentlichen Verwaltung. Sie erstellen eigene (modulare) Plattformen, auf denen Online-Dienste der Verwaltungen realisiert werden. Ihr Auftrag ist es, die Verwaltungsdienste portalverbundfähig zu gestalten und an der Interoperabilität und Vernetzung der verschiedenen Nutzerkonten mitzuwirken.

2. Ergebnisse der Debatte

Großer Bedarf am Management digitaler Identitäten

Einigkeit bestand unter den Teilnehmern darüber, dass von Seiten der Nutzer ein hoher Bedarf für ein übergreifendes Identitätsmanagement besteht, das Staat und Wirtschaft umfasst.

Dabei kommt es aus Sicht der Teilnehmer zum einen auf die Usability digitaler Authentifizierung und Identifizierung an. Nur wenn diese Dienste einfach nutzbar sind, finden sie auch Eingang in den Alltag der Menschen. Zum anderen bedürfen bestimmte Leistungen, die ein hohes Maß an Vertrauen erfordern, hohe Sicherheitsanforderungen. Dazu gehören auch viele Verwaltungsleistungen.

Der Staat vermag derzeit weder eine einheitliche digitale Identität für die Bürger anzubieten noch verfügt er über ein interoperables, alltagstaugliche digitales Identifizierungs- und Authentifizierungsinstrument. Lediglich in einzelnen Sektoren wie der Steuerverwaltung ist es mit der Steuer-ID gelungen, eine partielle digitale Identität zu schaffen. Der neue Personalausweis als wichtigstes staatliches digitales Identifizierungsinstrument hat nur eine sehr eingeschränkte Reichweite. Die Errichtung des Portalverbundes und der interoperablen Servicekonten löst das Grundproblem der fehlenden vertrauenswürdigen und einheitlichen digitalen Identität nicht.

Überdies hängt die Akzeptanz und Durchsetzung von einheitlichen Identifizierungsdiensten stark von der Nutzungshäufigkeit ab. Selbst bei der Zusammenführung aller staatlichen und kommunalen Leistungen im Portalverbund mit einheitlichem Nutzerkonto wird die Anzahl der Nutzungsvorgänge öffentlicher digitaler Dienste immer unterhalb der hierfür relevanten Schwelle bleiben.

Aufgrund der Verschränkungen zwischen öffentlichem Bereich und privater Wirtschaft, insbesondere auch der regulatorisch definierten

Identifizierungsvorgaben, wird es auch der Wirtschaft im Alleingang nicht gelingen, eine übergreifende digitale Identität zu etablieren. Es bietet sich daher an, strategische und architektonische Gemeinsamkeiten zu definieren und eine gemeinsame Identitäten-Strategie auf der Grundlage digitaler Plattformen zu entwickeln. Eine Kooperation zwischen Staat und Wirtschaft ist in dieser Hinsicht unabdingbar.

Offene Schnittstellen und Interoperabilität

Wesentlich aus Sicht der Workshop-Teilnehmer ist, dass Plattformen für digitale Identitäten für Staat und Wirtschaft interoperabel sein müssen, um einen hohen Nutzwert zu ermöglichen und eine niederschwellige Einbindung zu erlauben. Dabei gilt es Insellösungen zu vermeiden, da diese aufwendig und teuer und damit wenig erfolgversprechend sind. Durch die Implementierung von offenen und interoperablen Schnittstellen, die einen möglichst einheitlichen Standard haben, kann ein Identitätsmanagement erfolgen, welches sowohl für Staat und Wirtschaft nutzbar ist. Aus Sicht der Teilnehmer ist bislang keine strategische und architektonische Gemeinsamkeit definiert, auf der aufgebaut werden könnte.

Zukünftig wird daher entscheidend und erforderlich sein, eine gesamthafte Identitäten-Strategie zwischen Staat und Wirtschaft zu diskutieren und Rahmenbedingungen festzulegen, an denen sich Plattformen einerseits und die sie nutzenden Institutionen aus Staat und Wirtschaft andererseits orientieren können. Dabei wird auch die Weiterentwicklung einheitlicher Nutzerkonten in Richtung digitale Plattformen notwendig sein.

Von Seiten des Staates sollte darauf geachtet werden, dass keine überzogenen Anforderungen an die Einbindung solcher Plattformen in öffentliche Anwendungen gestellt werden, da eine Überregulierung die Verbreitung und Durchsetzung von notwendigen Plattformen für digitale Identitäten hemmen oder dem gar entgegenstehen könnte.

Regulierung digitaler Plattformen

Schon heute regulieren eine Vielzahl von europäischen und nationalen Vorgaben auch die Ausgestaltung digitaler Identitäts-Plattformen. Von besonderer Bedeutung sind dabei die Vorgaben der Datenschutzgrundverordnung (DSGVO), die die Datenhoheit der Nutzer stärken will, sowie die eIDAS-Verordnung, die Vorgaben zur Bereitstellung digitaler Identitäten und von Vertrauensdiensten macht. Daneben wird für Teile der potenziellen Nutzer auch Abbildung und Einhaltung der Vorgaben der bevorstehenden ePrivacy-Verordnung (für Onlinevermarkter) und der EU-Zahlungsdiensterichtlinie PSD II (für Zahlungsdienstleister) erforderlich. Letztere macht besondere Vorgaben für den sicheren Zugang zu Konten von Nutzern. Soweit staatliche Institutionen Nutzer der Plattformen sein sollen, sind neben dem OZG überdies auch die Vorgaben des Gesetzes zur Förderung der elektronischen Verwaltung (EGovG) und die bereichsspezifischen Fachgesetze zu beachten.

Aus all diesen Vorgaben ergibt sich schon heute ein enges regulatorisches Netz, das die Interessen des Einzelnen und der nutzenden Institutionen aus Staat und Wirtschaft in Einklang bringen. Zusätzliche Regulierungen von digitalen Plattformen bergen die Gefahr, so enge Grenzen zu setzen, dass die erforderliche Agilität und Dynamik bei der Weiterentwicklung von Plattformen für digitale Identitäten sowie der Wettbewerb unter Anbietern in Europa gefährdet sein kann. Weitere regulatorische Anforderungen könnten zudem schwer erfüllbare Hürden für kleine und mittelständische Unternehmen und Startups stellen. Daher sollten weitere Regulierung auf europäischer Ebene vermieden werden. Vielmehr gilt es zukünftig die bestehende Rechtslage gegenüber den tatsächlichen Erfordernissen abzugleichen und dort, wo ein besonderes Bedürfnis auf dem Weg zu einer Umsetzung und Einführung von Plattformen für digitale Identitäten besteht, die Rechtlage maßvoll zu ändern oder zu ergänzen.

Digitale Plattformen als Teil der Daseinsvorsorge und Einordnung als KRITIS

Viele Leistungen der Daseinsvorsorge werden bereits heute digital abgebildet, auch Leistungen der klassischen Daseinsvorsorge. Derzeit lässt sich noch nicht eindeutig feststellen, dass digitale Plattformen allgemein bereits Teil der Daseinsvorsorge sind, da die angebotenen Leistungen überwiegend auch noch analog verfügbar sind. Anders stellt sich die Beurteilung bei dem Identitätsmanagement dar. Ohne digitale Identitäten ist digitales Leben nicht möglich. Identitätsmanagementsysteme sind daher als Teil der Daseinsvorsorge zu betrachten.

Für eine Einordnung von Plattformen als Kritische Infrastrukturen ist es noch zu früh. Eine kritische Infrastruktur liegt nur dann vor, wenn das Angebot alternativlos ist. Das ist derzeit noch nicht der Fall. Einigkeit bestand bei den Workshop-Teilnehmern darüber, dass digitale Plattformen aufgrund der zur Verfügung stehenden Alternativen daher derzeit nicht als kritische Infrastrukturen einzuordnen sind. Im Hinblick auf ihre Bedeutung als querschnittliche digitale Dienste könnte jedoch eine Einordnung als digitale Dienste im Sinne der NIS-Richtlinie in Frage kommen, also eine Gleichstellung von Plattformen mit Suchmaschinen, Online-Marktplätzen und Cloud-Diensten.

Plattformdebatte Mobilität 4.0 – Juli 2018

Martin Schallbruch, Tanja Strüve und Isabel Skierka

Im Juli 2018 war das Digital Society Institute Gastgeber der Plattformdebatte Mobilität 4.0, die im Rahmen eines von Verimi initiierten Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen ausgerichtet wurde. Die Veranstaltung ging den Fragen nach, welche Rolle digitale Plattformen in der Förderung von der vernetzten „Mobilität 4.0“ einnehmen können und welche Anforderungen an digitale Plattformen zum Identity Management in der Mobilität 4.0 bestehen. Impulse zu der Debatte trugen MinDirig Andreas Krüger (Bundesministerium für Verkehr und digitale Infrastruktur), Dr. Julius Rauber (ConPolicy), Graham Smethurst (Verband der Automobilindustrie) und Dr. Jeannette von Ratibor (Verimi GmbH) bei.

1. Sachstand

Chancen und Herausforderungen der Mobilität 4.0

Die digitale Transformation eröffnet große Potentiale für die Mobilität der Zukunft. Die stärkere Vernetzung der Verkehrsträger untereinander sowie der zunehmende Einsatz von IT in Verkehrs- und Logistikprozessen eröffnen neue Möglichkeiten für Innovation und Verbesserung der Planung und Effizienz von Transport und Verkehr. Zugleich steht die Mobilität der Zukunft vor großen Herausforderungen. Es gilt, die Klimaschutzziele zu erreichen. Dazu werden auf den Ausbau der E-Mobilität und des Radverkehrs gesetzt und zugleich Sharing-Modelle gefördert. Darüber hinaus gilt es, den Mobilitätsbedürfnissen der Nutzer individueller gerecht zu werden und gleichzeitig die Verkehrsinfrastrukturen der Ballungsräume zu entlasten und Mobilitätsangebote auf dem Land zu gewährleisten.

Stärkere Automatisierung durch Digitalisierung

Ein wichtiger Bereich der Mobilität 4.0 ist das assistierte, automatisierte und vernetzte Fahren. Vernetztes Fahren umfasst zum einen die Fahrzeug-zu-Fahrzeug Kommunikation sowie die Kommunikation zwischen Fahrzeugen und der Straßen- und Verkehrsinfrastruktur. Bereits heute sind zahlreiche semi-autonome Fahrzeuge auf den Straßen unterwegs. Softwarefirmen entwickeln seit über einem Jahrzehnt selbstfahrende Autos. Selbstfahrende Systeme beschränken sich nicht auf Autos, sondern umfassen auch Nutzfahrzeuge, Schienen-, Luft- und Wasserfahrzeuge. In der Landwirtschaft wird bereits satellitengestützte Navigationstechnik eingesetzt; die Metro in Dubai fährt vernetzt und seit April 2018 wird in Deutschland im Rahmen eines Forschungsprojektes auf der Autobahn BAB 9 *Platooning* getestet. Bei diesem digital vernetzten Konvoi werden Lkw per Funk gesteuert und fahren in einem Abstand von 12 bis 15 Metern hintereinander her. Neben dem digitalen Testfeld der Autobahn BAB 9 werden zur Erprobung im Realverkehr weitere Testfelder in Städten wie u.a. in Berlin, Hamburg, Düsseldorf, Braunschweig und München sowie länderübergrei-

fende Testfelder zwischen Deutschland, Frankreich und Luxemburg genutzt[6]. Zukünftig sind zudem digitale Testfelder im Bereich Schiene, Wasserstraße und in Häfen geplant. Um die Automatisierung und Vernetzung des Verkehrs weiter auszubauen, bedarf es als Grundvoraussetzung einer ausreichenden flächendeckenden Netzabdeckung.

Berücksichtigung individueller Mobilitätsbedürfnisse der Nutzer

Während der Fokus der Mobilität um die Jahrtausendwende auf dem Individualverkehr lag, ist zunehmend eine Tendenz zur Nutzung von öffentlichen und Sharing-Angeboten zu erkennen. Die Erwartung der Nutzer ist gleichwohl ein den individuellen Bedürfnissen entsprechendes Angebot. Dementsprechend sind Mobilitätsangebote immer mehr auf „Mobility on demand" für den Nutzer ausgerichtet. Wie die Studie „Zur Zukunft der Mobilität 2025" des Münchner Kreises darlegt, stehen momentan noch verschiedene Mobilitäts-Modelle, z.B. die Nutzung öffentlicher versus privater Mobilitätsangebote oder der Besitz von Verkehrsmitteln wie Auto, Fahrrad oder Roller versus Sharing weitgehend unverbunden nebeneinander. In der Praxis kombinieren Nutzer diese Angebote schon jetzt zunehmend. Eine Herausforderung für die Anbieter von Mobilitätsdiensten besteht daher in der Kombination und Integration verschiedener Modelle in übergreifenden Angeboten.[7]

Big Data in der Mobilität

Eine weitere übergreifende Herausforderung in der Mobilität 4.0 ist der Umgang mit Daten im Mobilitätsbereich. Nutzer generieren ständig Mobilitätsdaten – u.a. im Fahrzeug, bei der Routenplanung, beim Kauf von Verkehrstickets und bei der Nutzung von Sharing-Angeboten. Diese Daten wiederum können vielfältigen Zwecken dienen. Sie können als Ressource zur Planung individualisierter Angebote ebenso wie zur Steuerung des Verkehrsflusses oder für die Schaffung neuer Infrastrukturen verwendet werden. Auch die Nutzer selbst könnten ihre Daten für eigene Zwecke einsetzen. Daher stellt sich die Frage, wer diese Daten zu welchem Zweck verwenden darf und wie die Rechte der Nutzer praktisch gewahrt werden können (Datenschutzkonzept). Um diese Daten vor unberechtigtem Zugriff zu schützen, ist zudem eine hinreichende Datensicherheit zu gewährleisten. Die Daten sind gegen Verlust, Manipulation, Ausspähung und andere Bedrohungen zu schützen.

Digitale Plattformen in der Mobilität 4.0

Es gibt eine Vielzahl von digitalen Angeboten in der Mobilität. Viele Angebote sind noch in frühen Stadien. Ein Markt digitaler Mobilitätsangebote kann derzeit noch schwer beschrieben werden. Digitale Plattformen nehmen bereits heute eine zunehmend zentrale Rolle ein. Sie fungieren als Marktplatz, auf dem verschiedene Anbieter ihre Produkte und Dienste an Kunden anbieten und dabei auch miteinander konkurrieren. Zum anderen offerieren einige Plattformen dem Kunden auch selbst ein Angebot einer durchgängigen Mobilitätskette.[8]

Einige Plattformen im Mobilitätsbereich integrieren bereits verschiedene Mobilitätsangebote der Sharing Economy. Dienste wie *Here* oder *Google Maps* bieten Routenplanung mit verschiedenen Verkehrsmitteln an. Auch der Staat betreibt Plattformen im Bereich Mobilität. Die vom Bundesministerium für Verkehr und digitale Infrastruktur initiierte neutrale B2B Plattform *MDM* fungiert als Marktplatz für Mobilitätsdaten und stellt als zentrales Online-Portal Verkehrsdaten wie beispielsweise Informationen zu Verkehrsströmen, Staus, Baustellen, Parkmöglichkeiten u.a bereit[9].

Das Projekt *OPA_TAD* des BMVI will den Umgang mit großen Datenmengen verbessern. Dazu soll eine Big-Data-Infrastruktur aufgebaut werden, mit deren Hilfe große Datenmengen im ersten Schritt strukturiert und im weiteren Schritt

[6] Bundesministerium für Verkehr und digitale Infrastruktur; https://www.bmvi.de/DE/Themen/Digitales/Digitale-Testfelder/Digitale-Testfelder.html

[7] Muenchner Kreis. (2017). Zur Zukunft der Mobilität 2025. Zukunftsstudie Münchner Kreis Band VII. https://www.muenchner-kreis.de/download/zukunftsstudie7.pdf

[8] Vgl. Muenchner Kreis. (2017). Zur Zukunft der Mobilität 2025. Zukunftsstudie Münchner Kreis Band VII. https://www.muenchner-kreis.de/download/zukunftsstudie7.pdf

[9] https://www.mdm-portal.de/

eine Data-Science-Plattform implementiert werden, welche die Daten analysiert und daraus Informationen für den Nutzer generiert[10].

Eine weitere Plattform des BMVI ist *Cartox*. Diese Plattform für vernetztes und automatisiertes Fahren erfasst und verarbeitet Informationen über die Car-2-Car-Konnektivität.[11]

2. Rolle und Verantwortung von digitalen Plattformen in der Mobilität 4.0

Erfordernis einer digitalen Identität im Bereich Mobilität

Insbesondere in den Ballungsräumen gibt es eine Vielzahl von Anbietern von geteilten Mobilitätsdienstleistungen, von Angeboten des ÖPV/ÖPNV bis hin zu Sharing Modellen für Fahrräder, Roller oder Autos. Zur Nutzung dieser Mobilitätsangebote bedarf es einer verlässlichen Identifizierung und Authentifizierung. Dazu ist eine digitale Identität notwendig. Mit ihr lassen sich die Planung, Bestellung und auch Abrechnung von Mobilitätsangeboten abwickeln, Nutzer können den Nachweis erbringen, dass sie eine Nutzungsberechtigung haben. Darüber hinaus können Anbieter Angebote einer Mobilitätskette individualisieren. Im Mobilitätsbereich werden heute typischerweise unterschiedliche digitale Identitäten bei verschiedenen Mobilitätsanbietern verwendet, mit denen man sich nach einer initialen Identifizierung für jede Nutzung verlässlich authentifizieren muss. Für den Ausbau geteilter Mobilitätsangebote und verkehrsmittelübergreifende Planung und Nutzung ist diese Situation nicht zukunftsfähig.

Mobilitätsplattformen und digitale Identität

Bereits heute existieren Kooperationen von Plattformen mit Mobilitätsdienstleistern im Bereich der *Mobility on demand*: u.a. die Berliner Verkehrsbetriebe mit ViaVan, die Hamburger Hochbahn mit MOIA oder die Duisburger Verkehrsbetriebe mit Door2Door. Eine Mobilitätsplattform mit ganzheitlichen und übergreifenden Mobilitätslösungen gibt es derzeit nicht. Im Koalitionsvertrag der jetzigen Bundesregierung haben sich die Parteien darauf verständigt, eine digitale Mobilitätsplattform einzuführen, auf der Mobilität über alle Fortbewegungsmittel (z.B. Auto, ÖPNV, E-Bikes, Car- und Ride-Sharing, Ruftaxen) hinweg geplant, gebucht und bezahlt werden kann.[12] Eine einheitliche Mobilitätsplattform kann so ausgestaltet sein, dass sie dem Kunden ein Angebot einer durchgängigen Mobilitätskette unterbreitet, die verkehrsmittelübergreifend ist. Kunden hätten so einen Einblick in die Verfügbarkeit und ggfs. die Qualität aller Mobilitätsangebote. Zugleich würde sie Car- und Ridesharing sowie die Nutzung des ÖPV und ÖPNV und weiterer Möglichkeiten erleichtern. Eine solche Plattform sollte nach Möglichkeit leicht bedienbar sein, individualisierte Angebote bereithalten und Anbieter- und Verkehrsmittel-übergreifend funktionieren.

Voraussetzung hierfür ist die Integration einer digitalen Identität in die Plattform, die über unterschiedliche Anbieter (und deren Identitätsdienste) hinaus reicht im Sinne eines Single-Sign-On sowie der Planung, Buchung und Abrechnung individualisierter Mobilitätsangebote.

Umgang mit Mobilitätsnutzungsdaten

Verkehrsdaten und Nutzerdaten von Fahrzeugen haben eine herausragende Bedeutung für die Zukunftskonzepte der Mobilität, sei es, um eine smarte Verkehrsführung zu etablieren oder dem Nutzer ein individuell auf ihn zugeschnittenes Mobilitätsangebot zu unterbreiten. Insbesondere bei

[10] http://www.bmvi.de/SharedDocs/DE/Artikel/DG/mfund-projekte/offene-plattform-fuer-verkehrsprognosen-opatad.html

[11] https://www.bmvi.de/SharedDocs/DE/Artikel/DG/mfund-projekte/serviceplattform-c2c-kommunikation-cartox2.html

[12] Koalitionsvertrag CDU/CSU und SPD, Rn. 2133-2141

den Nutzungsdaten aus einem Kfz wirft die Verwendung solcher Daten hingegen auch Interessenkonflikte auf. Die im vernetzten Auto generierten Daten sind von großem Interesse für Hersteller, Werkstätten, staatlichen Stellen wie Gerichten und Strafverfolgungsbehörden. Aber auch für Produktanbieter oder Dienstleister sind die Daten von hohem Interesse, zum Beispiel Kfz-Versicherungen, die aufgrund der erhobenen Fahrzeugdaten einen individuell zugeschnittenen Versicherungsbeitrag, einen sogenannten telematikbasierten Versicherungstarif, anbieten.

Bei einem zunehmend digitalen und vernetzten Fahrzeug entstehen eine Fülle von unterschiedlichen Daten, die sowohl sehr nah an dem Verhalten des Fahrzeugführers sein können wie auch sehr nah an den technischen Funktionalitäten des Fahrzeugs. Aufgrund der Vielzahl von Datenarten und der Datenmenge ist dabei für den Eigentümer, Halter oder Fahrer eines Fahrzeuges nicht ohne weiteres transparent zu machen, welche Daten erhoben und zu welchem Zweck sie verwendet werden. In rechtlicher und politischer Hinsicht wirft die Nutzung der Daten aus Fahrzeugen viele Fragen auf: Wem gehören die Fahrzeugdaten im zivilrechtlichen Sinne? Welche Auswirkungen hat die Nutzung der Daten auf das Recht auf informationelle Selbstbestimmung oder auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme?[13] Soweit angenommen wird, dass es sich bei fahrzeugbezogenen Daten um personenbezogene Daten handelt, bedarf es zur Rechtmäßigkeit ihrer Verarbeitung einer der in Artikel 6 DSGVO normierten Erlaubnistatbestände. Regelmäßig wird dies die Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO sein, die beim Kauf des Kfz erteilt wird. Auf die vom Fahrzeug generierten Daten, zumeist sensiblen und zumindest personenbeziehbaren Daten oder personenbezogenen Daten, haben Eigentümer, Halter oder Fahrer des Fahrzeuges in der Regel keinen Zugriff. Fraglich ist, wie eine vertrauenswürdige Verwaltung der sensiblen Daten aussehen kann und wie die Sicherheit des Fahrzeuges im Hinblick auf digitale Zugriffe von außen gewährleistet werden kann. Hierfür bestehen unterschiedliche Konzepte, wie die Verantwortung für den Datenzugriff zwischen Fahrer/Halter, OEM und weiteren Interessenten aufgeteilt und technisch-organisatorisch abgesichert werden kann.

Standardisierte Schnittstellen und Interoperabilität

Plattformen für digitale Mobilitätsangebote sollten schon wegen des Bedürfnisses der Nutzer nach individueller Anbieter- und Verkehrsmittel-übergreifenden Mobilitätslösungen möglichst interoperabel mit Diensten von Anbietern sowie mit anderen Plattformen sein. Die technische Offenheit einer Plattform durch offene Standards erleichtert die Verknüpfung von Angeboten und senkt die Markteintrittshürde für Diensteanbieter. Sie ist somit auch aus marktwirtschaftlicher Perspektive vorteilhaft. Einheitliche und interoperable Datenformate ermöglichen zudem die vielfältige Auswertung und Nutzung von Mobilitätsdaten durch verschiedene Anbieter zur Verbesserung der Qualität von Verkehr und Infrastruktur sowie für den Nutzer zur Stärkung der eigenen digitalen Souveränität im Bereich der Mobilität.

[13] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350.

Plattformdebatte Interoperabilität, Offenheit und Datenportabilität – August 2018

Martin Schallbruch, Isabel Skierka und Tanja Strüve

Am 28. August 2018 war das Digital Society Institute Gastgeber der Plattformdebatte Interoperabilität, Offenheit und Datenportabilität, die im Rahmen eines Begleitforschungsprojektes für die Verimi GmbH zur gesellschaftlichen Verankerung digitaler Plattformen ausgerichtet wurde. Im Rahmen der Veranstaltung sollte der Frage nachgegangen werden, welche Anforderungen sich im Hinblick auf Interoperabilität und offene Standards für digitale Plattformen ergeben. Darüber hinaus diskutierten Teilnehmer darüber, welche Rolle digitalen Plattformen als Betroffene von Datenportabilitäts-Anforderungen zukommt und wie sie Nutzer und Anbieter bei der Umsetzung von Datenportabilität unterstützen können. Impulse zu der Debatte trugen Frederik Richter (Stiftung Datenschutz), Susanne Dehmel (Bitkom), Cord Bartels (Beauftragter des BSI) und Dr. Dirk Woywod (Verimi GmbH) bei.

1. Sachstand

Interoperabilität im Kontext digitaler Plattformen

Allgemein bezeichnet Interoperabilität die Fähigkeit unabhängiger, heterogener Systeme, möglichst nahtlos zusammenzuarbeiten. Dadurch können wechselseitig Funktionen und Dienste genutzt werden, um Informationen auszutauschen.[14] Grundvoraussetzung für Interoperabilität auf der technischen Ebene (syntaktische Interoperabilität) sind gemeinsame Schnittstellen und gemeinsame (möglichst offene) Standards. Offene Standards sind Formate oder Protokolle, die für alle Marktteilnehmer leicht zugänglich und frei von rechtlichen oder technischen Einschränkungen sind und leicht verwendet und weiterentwickelt werden können.

Semantische Interoperabilität, welche sicherstellt, dass ausgetauschte Daten für beteiligte Anwendungen und Akteure die gleiche Bedeutung haben, ist im Kontext von digitalen Produkten und Diensten ebenfalls von hoher Priorität. Darüber hinaus gelten für die Verwendung von Daten und für den Ablauf von Geschäftsprozessen in der digitalen Wirtschaft organisatorische und rechtliche Dimensionen von Interoperabilität.

Die Interoperabilität von Netzwerken, Geräten, Applikationen und digitalen Diensten ist ein Grundbaustein für die Digitalwirtschaft. Daher ist die Förderung von Interoperabilität digitaler Technologien und Dienste Kernziel der Digitalen Agenda der EU. Insbesondere mit Hinblick auf digitale Plattformen, die stetig an Bedeutung als Organisationsformen der Gesellschaft und Wirtschaft gewinnen, ist die Frage nach deren Interoperabilität mit anderen digitalen Diensten und Plattformen virulent.

Interoperabilität ist kein binärer Zustand, sondern immer eine Frage des Grades. Mit Hinblick

[14] Deutscher Bundestag. (2013). Zehnter Zwischenbericht der Enquete-Kommission „Internet und digitale Gesellschaft" - Interoperabilität, Standards, Freie Software. Drucksache 17/12495.

auf digitale Plattformen muss unterschieden werden zwischen horizontaler und vertikaler Interoperabilität von Diensten und Plattformen.[15] Horizontale Interoperabilität bezeichnet die Interoperabilität von konkurrierenden Produkten, Diensten und Plattformen. Ein Beispiel sind Plattform-übergreifende Single-Sign-On (SSO)- Lösungen oder die (mangelnde) Interoperabilität von Messenger-Diensten. Vertikale Interoperabilität bezeichnet die Interoperabilität eines Produkts, Dienstes oder einer Plattform mit komplementären Produkten oder Diensten. Je höher der Grad, zu dem unabhängige Firmen Produkte auf einer Plattform anbieten können, desto höher die vertikale Interoperabilität der Plattform. Beispiele sind Amazon Marketplace oder das Facebook-Profil, über das sich Anbieter und User verknüpfen können.

Insgesamt ist Interoperabilität im digitalen Raum kein absoluter Wert an sich, sondern hat sowohl Vorteile als auch Nachteile. Zu den Vorteilen gehört die Möglichkeit für Nutzer, ohne hohen technischen und finanziellen Aufwand die Plattform zu wechseln, oder – im Bereich E-Government – Daten zwischen Behörden austauschen und verknüpfen zu können. Interoperabilität von Komponenten, Systemen und Prozessen ist außerdem ein Katalysator für Innovation, da es Insellösungen vermeidet, die wenig effizient und innovationsfeindlich sind. Außerdem kann Interoperabilität zu einer Stärkung des Wettbewerbs zwischen Angeboten und Plattformen beitragen, was wiederum zu einer Senkung der Kosten für Kunden führen kann.

Ein Nachteil von hoher oder voller Interoperabilität und uniformen Standards ist das Risiko einer größeren Homogenität von Diensten und Produkten. Der Druck der Kompatibilität mit einheitlichen Standards und Anforderungen kann Möglichkeiten zur Entwicklung eigener spezifischer, differenzierter Produkte und Dienste verringern, insbesondere für kleinere Firmen. Dadurch kann wiederum Innovation eingeschränkt werden. Die Offenheit von Plattformen für unterschiedliche Angebote kann auch Qualitäts- und Sicherheitsrisiken mit sich bringen, wenn diese nicht ausreichend geprüft sind.[16] Eine Vorschrift zur Interoperabilität von digitalen Plattformen ist also nur unter einschränkenden Bedingungen sinnvoll.

Insgesamt bringt Interoperabilität zwischen Produkten, Diensten und Plattformen grundsätzlich viele Vorteile für die Digitalwirtschaft, Unternehmen und Nutzer und sollte daher, unter Beachtung der beschriebenen Randbedingungen, allgemein angestrebt werden.

Interoperabilität digitaler Identitäten

Digitale Identitäten sind zur Teilhabebedingung in der digitalen Welt geworden. Proprietäre oder auf einzelne Dienste bezogene Lösungen sind sowohl für Anbieter von Diensten wie auch für Nutzer unattraktiv. Immer häufiger nehmen sie für die Verwaltung von Nutzerkonten Identitäts-Management-Systeme in Anspruch. Der Bedarf an digitalen Identitäten steigt insbesondere im mobilen Bereich an und hat dort mittlerweile jenen an Desktopangeboten überholt.

Die übergreifende Verwaltung von Identitäten durch Plattformen setzt ein gewisses Maß an vertikaler Interoperabilität mit verschiedenen komplementären Angeboten voraus und kann auch horizontale Interoperabilität mit anderen Plattformen fördern. Dazu bedarf es interoperabler Schnittstellen und Standards.

Ein offener Standard, der sich als dezentrales Authentifizierungssystem für webbasierte Dienste etabliert hat, ist das OpenID Connect Protokoll, welches wiederum auf OAuth 2.0 basiert. Es ermöglicht Funktionen für SSO und wird auch von Plattformen wie Facebook, Google und Verimi implementiert.

Die deutsche Bundesregierung und 19 Partner aus dem Privatsektor haben mit dem OPTIMOS 2.0-Projekt eine Initiative gestartet, um ein eIDAS-konformes Ökosystem für mobile Dienste zu schaffen. OPTIMOS 2.0 ist offen und implementiert internationale Standards. Der Sicherheit des

[15] Schweitzer, H., & Kerber, W. (2017). Interoperability in the digital economy. *MACIE Paper Series*.

[16] Schweitzer, H., & Kerber, W. (2017). Interoperability in the digital economy. *MACIE Paper Series*.

Dienstes kommt eine hohe Bedeutung zu, weswegen das BSI sich im OPTIMOS-Projekt besonders engagiert. OPTIMOS ist geeignet, grundlegende Interoperabilitätsvoraussetzungen zu schaffen. Im Hinblick auf die Nutzung und Bereitstellung digitaler Identitäten durch Plattformen sind darüber hinaus zusätzlich organisatorische und rechtliche Fragen interoperabler Identitäten zu beantworten.

Datenportabilität in der Praxis

Insbesondere für die Datenübertragbarkeit spielt Interoperabilität eine wichtige Rolle. Nutzer hinterlassen bei digitalen Diensten personenbezogene Daten. Bei der Nutzung anderer konkurrierender Dienste stellt sich für die Nutzer die Frage, ob und wie sie ihre bereits bei anderen Dienstanbietern generierten und gespeicherten Daten zu anderen Anbietern migrieren können.

Das Recht auf Datenportabilität hat mit der verbindlichen Geltung der DSGVO seit dem 25. Mai 2018 Einzug in das europäische Recht gefunden. Nach Art. 20 DSGVO haben Nutzer das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen, maschinenlesbaren Format zu erhalten. Aus Erwägungsgrund 68 geht hervor, dass dem Nutzer mithilfe dieser Norm eine bessere Kontrolle über die eigenen Daten verliehen werden soll, indem er die Datenmigration von einem zum anderen Anbieter verlangen kann. Vom Recht auf Migration der eigenen Daten sind dabei lediglich die vom Nutzer „bereitgestellten" Daten umfasst. Nach Ansicht der Aufsichtsbehörden unterfallen dem Begriff „bereitstellen" auch Daten, welche indirekt bereitgestellt wurden, bspw. Daten aus Smart Metern oder Fitnesstrackern.[17] Die Ausübung des Rechts auf Datenportabilität führt dabei gleichzeitig zu einer Vervielfältigung der Nutzerdaten, da mit dem Recht auf Datenportierung nicht gleichzeitig das Recht auf Löschung der Daten beim ersten Anbieter einhergeht. Ein Anspruch auf Löschung der Daten ergibt sich aus Art. 17 DSGVO, wenn die Voraussetzungen nach dieser Norm vorliegen. Aufgrund der mit der Datenportabilität in der Regel einhergehende Datenmultiplizierung erhöht sich im gleichen Maße auch das Risiko der Datensicherheit in Bezug auf die übertragenen Daten. Ein besonderes Risiko ergibt sich nicht nur aus der reinen Multiplizierung, vielmehr besteht ein Risiko auch in dem Übertragungsvorgang als solchen.

Weiterhin folgt aus dem Anspruch auf Datenportabilität kein Anspruch auf die Zurverfügungstellung der Daten in einem besonderen oder von dem Nutzer gewünschten Format. Die DSGVO ist technologieneutral und macht keinerlei Vorgaben an Formate und Standards. Die Stiftung Datenschutz schlägt daher als Umsetzung der Datenportabilität die Erarbeitung von branchenspezifischen Umsetzungsstrategien und Standards für die Datenportabilität im Sinne der „regulierten Selbstregulierung" vor.[18]

Ein erstes Beispiel für eine großflächige Umsetzung von Datenportabilität durch digitale Plattformen ist das Data Transfer Projekt (DTP), eine Initiative von Google, Microsoft, Twitter und Facebook. Das DTP stellt offene Software-Adapter bereit, die es beliebigen Online-Dienstleistern ermöglichen, eine nahtlose, direkte und benutzerinitiierte Portabilität von Daten zwischen beiden Plattformen umzusetzen. Entscheidend ist dabei, dass heterogene Standards bestehen bleiben und mithilfe der Adapter in standardisierte Formate umgewandelt werden können, damit diese dann der Zielplattform übergeben werden können.

Datenportabilität erfordert also ein gewisses Maß an Interoperabilität zwischen verschiedenen Datenformaten. Dadurch werden zwar die Netzwerkeffekte dominanter Plattformen nicht überwunden, aber Lock-In-Effekte abgeschwächt. Durch die Erhöhung der Nutzermobilität erleichtert sie einen Übergang zu überlegenen Alternativen.

[17] Article 29 Data Protection Working Party. (2017). Guidelines on the Right to Data Portability, WP 242rev.01 (adopted on 5 April 2017). 10.

[18] Stiftung Datenschutz. (2018). Praktische Umsetzung des Rechts auf Datenübertragbarkeit.

2. Ergebnisse der Debatte

Anforderungen an Interoperabilität von Plattformen

Um erfolgreich anbieterübergreifend zu funktionieren, sollten Plattformen möglichst interoperabel mit komplementären Produkten und Diensten sein. Damit wird die Integration neuer Anwendungspartner und die Erweiterung der Dienste erleichtert. Dabei sollte darauf geachtet werden, dass diese Mindeststandards für Qualität und Sicherheit erfüllen, die regelmäßig überprüft werden.

Eine Verpflichtung zur vollen Interoperabilität ist aufgrund der oben genannten Risiken für Innovation, Marktdifferenzierung und Qualität der Angebote nicht empfehlenswert. Vielmehr sollten Plattformen und Anbieter einheitliche Standards untereinander verhandeln.

Eine weitere Möglichkeit besteht darin, dass der Staat die Herstellung von Interoperabilität vorgibt (wie zum Beispiel durch PSD II), um Märkte zu öffnen. Wegen der hohen Eingriffsqualität muss hierbei eine sorgfältige Prüfung erfolgen. Der Staat kann zudem eine unterstützende Rolle spielen oder selbst Projekte anstoßen und mit Anbietern kooperieren.

Bei der Schaffung von Interoperabilität sollte außerdem auf die Ebene geachtet werden, auf der diese implementiert werden sollte. Zum Beispiel ist die Implementierung von Interoperabilität auf Protokollebene zur Weitergabe von Daten in Form von verified credentials gewinnbringend für die meisten Akteure, insbesondere mit Hinblick auf Datenportabilität.

Ein Bereich, in dem die Schaffung von Interoperabilität sinnvoll wäre, findet sich bei Messenger-Diensten. Jedoch ist eine volle Interoperabilität von Messenger-Diensten untereinander nicht leicht mit der implementierten Ende-zu-Ende-Verschlüsselung bei vielen Messengern zu vereinbaren.

Interoperable Digitale Identitäten

Für einen hohen Nutzwert sollten elektronische Identitäten einen diskriminierungsfreien Zugang zu Diensten und universelle Anwendbarkeit ermöglichen. Dazu bedarf es interoperablen Lösungen, die auf einheitlichen Protokollen und offenen Schnittstellen basieren.

Tatsächlich ist die Umsetzung von Interoperabilität in geschlossenen proprietären Systemen einfacher, da Standards und Spezifikationen unilateral und effizient vom Systembesitzer durchgesetzt werden können. Es erlaubt dem Systembetreiber auch, eigene Standards für Datenschutz und Sicherheit zu setzen, wodurch Lock-In Effekte entstehen und Tracking und Datensammlung über Nutzer ermöglicht werden können.

Einen diskriminierungsfreien Zugang zu Angeboten, mehr Auswahl für Kunden sowie die Einhaltung von „state of the art“ Datenschutz- und IT-Sicherheitsanforderungen ermöglichen offene eID-Ökosysteme. Grundsätzlich sollte Interoperabilität daher in offenen eID-Ökosystemen umgesetzt werden. Diese erfordern jedoch ein höheres Maß an Abstimmung und entsprechende Lösungen müssen skalierbar sein.

Zudem müssen digitale Identitäten vertrauenswürdig sein und je nach Schutzprofil unterschiedliche Sicherheits-Niveaus gewährleisten. Um eine breite Anwendung auf dem europäischen Markt für Anwendungen im privaten sowie öffentlichen Sektor zu ermöglichen, sollten diese interoperablen Identitäts-Lösungen konform mit eIDAS-Kriterien sein. Ein Beispiel ist das oben genannte OPTIMOS 2.0-Projekt, welches skalierbare eIDAS-konforme eID-Dienste anbieten wird.

Entsprechende Standards sollten gemeinsam mit allen beteiligten Stakeholdern, insbesondere mit den Herstellern mobiler Geräte und Betriebssysteme, erarbeitet werden. Denn fortgeschrittene Sicherheitsanforderungen lassen sich nur mit einem entsprechenden Sicherheitselement im Mobilgerät umsetzen.

Das Beispiel von Apples Widerstand gegen die Öffnung der NFC-Schnittstelle des iPhones für Dritte ist sinnbildlich dafür, wie ein Gerätehersteller die Interoperabilität von Identitäts-Lösungen verringern kann. Ein wachsender Bedarf für interoperable Identitäts-Lösungen in anderen

Märkten, wie zum Beispiel dem digitalen Zahlungsmarkt, kann jedoch den Druck auf Plattformbetreiber zur Öffnung erhöhen. Außerdem kann eine Öffnung auch staatlich erzwungen werden (siehe PSD II).

Herausforderungen im Hinblick auf Datenportabilität

Damit der Nutzer sein Recht auf Datenmitnahme auch geltend machen kann, müsste der in Art. 20 DSGVO festgeschriebene Anspruch, für den Nutzer auch tatsächlich umsetzbar sein. Eine Stärkung des Nutzerrechtes auf Mitnahme der eigenen Daten wird nur dann in der Praxis umsetzbar sein, wenn der Anbieter, zu dem die Daten migriert werden sollen, diese auch auslesen kann. Aus dem Anspruch auf Datenportabilität folgt nicht gleichsam ein Anspruch auf Angleichung der technischen Systeme. In der Praxis besteht daher das Problem, dass die Daten in dem bereitgestellten Format von einem anderen Diensteanbieter nicht ausgelesen werden und somit für den Nutzer nicht weiterverwendet werden können. Software-Adapter oder Konverter sind hier ein möglicher Lösungsansatz. Gleichsam können Rechte Dritter entgegenstehen. So können beispielsweise die mit einem Facebook-Account verknüpften Dritten mit der Datenmitnahme ihrer personenbezogenen Daten nicht einverstanden sein, beispielsweise von Fotos, auf denen sie selbst abgebildet sind.

Zudem ergibt sich eine Herausforderung aus der fehlenden Rechtssicherheit dahingehend, auf welche Daten sich der Herausgabeanspruch konkret bezieht. Findet die Datenportabilität beispielsweise auch auf Daten Anwendung, die bereits der PSD II unterliegen und modifiziert den dortigen Herausgabeanspruch? Oder verdrängt PSD II als Spezialregelung den Art. 20 DSGVO?

Aus dem der Arbeit der Bundesregierung zugrundeliegenden Koalitionsvertrag geht der Wille zur Stärkung des Rechtes auf Datenportabilität hervor. In der Praxis dominiert indes das Momentum des Abwartens; in der deutschen Wirtschaft gibt es keine vergleichbaren Projekte wie das Data Transfer Project und überdies kennen viele Nutzer ihren Anspruch auf Datenportabilität nicht.

Weitestgehende Einigkeit bestand unter den Teilnehmern darüber, dass man sich zur Umsetzung der Datenportabilität auf die zumindest partielle Interoperabilität von Diensten und Plattformen konzentrieren muss. Eine europäische Initiative hierzu wäre empfehlenswert, damit die Definition nicht den internationalen Industrieinitiativen überlassen wird. Ähnlich wie in OPTIMOS, der Plattform Industrie 4.0 oder der Initiative Industrial Data Space könnte ein wirtschaftsgetriebener, vom Staat unterstützter Ansatz der Definition eines Datenaustauschmodells entwickelt werden.

In diesem Zusammenhang könnte sich auch die Möglichkeit von neuen Geschäftsmodellen ergeben. Personal Information Management Services (PIMS) können beispielsweise Anbieter und Nutzer bei der Verwaltung persönlicher Daten und der Umsetzung von Datenportabilität als „zwischengeschaltete Instanz“ unterstützen.

Plattformdebatte Datensouveränität und Datenschutz-Management – September 2018

Tanja Strüve und Isabel Skierka

Am 12. September 2018 fand an der ESMT die Plattformdebatte Datensouveränität und Datenschutz-Management statt, die im Rahmen eines Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen ausgerichtet wurde. Im Rahmen der Veranstaltung sollte der Frage nachgegangen werden, inwieweit digitale Plattformen Nutzer dabei unterstützen können, die eigenen Daten selbstbestimmt und eigenständig zu verwalten und auf diese Weise die Datensouveränität jedes einzelnen zu stärken. Impulse zu der Debatte trugen Prof. Dr. Johannes Caspar (Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit), Luise Kranich (Forschungszentrum Informatik), Linus Neumann (Chaos Computer Club), Luc Mader (luckycloud GmbH) und Torsten Sonntag (VERIMI GmbH) bei.

1. Sachstand

Datenschutz in Zeiten von „Big Data

Digitale Plattformen als Organisationsformen der digitalen Gesellschaft und Wirtschaft gewinnen zunehmend an Bedeutung. Soziale Netzwerke wie Facebook[19], WhatsApp[20] oder Twitter[21] gehören zum Alltag vieler Menschen. Digitalisierte Dienste haben „alte Märkte“ abgelöst; Reisen werden über Internetplattformen gebucht, Einkäufe werden über Online-Händler wie Amazon[22] und Geldtransaktionen über Paypal[23] getätigt. Die Nutzung dieser Angebote steigt stetig; bei der Abwicklung von Rechtsgeschäften im Internet oder der Nutzung sozialer Netzwerke hinterlassen Nutzer große Datenvolumina im Netz. Im Jahr 2015 hatten Internet-Nutzer durchschnittlich 90 verschiedene Accounts. Schätzungen zufolge sollen es im Jahr 2020 durchschnittlich 200 Accounts pro Nutzer sein.[24] Hochgerechnet auf das Datenvolumen schätzen Experten von IBM und der Universität Berkley das weltweite Datenvolumen im Jahr 2020 auf 43 Zetabyte[25].

Für die moderne Digitalwirtschaft werden Daten zunehmend zu einer zentralen kritischen Ressource. Welche Daten sind das und wozu dienen sie? Die Datenspuren, die wir im Netz hinterlassen sind vielfältig. Dazu gehören beispielsweise Daten

[19] Juni 2018: durchschnittlich 1,47 Milliarden aktive Facebook täglich: Facebook: https://newsroom.fb.com/company-info/
[20] Im Jan 2018 nutzen 1,5 Milliarden Personen WhatsApp weltweit: https://de.statista.com/statistik/daten/studie/.../aktive-nutzer-von-whatsapp-weltweit/
[21] Im 3. Quartal 2018 hatte Twitter monatlich 326 Millionen aktive Nutzer: https://de.statista.com/statistik/daten/studie/232401/umfrage/monatlich-aktive-nutzer-von-twitter-weltweit-zeitreihe/
[22] 2015: Anzahl weltweit aktiver Kunden Accounts 300 Mio: https://de.statista.com/themen/757/amazon/
[23] 2. Quartal 2018: 244 Millionen PayPal-Accounts, mit denen innerhalb der letzten zwölf Monate Transaktionen getätigt wurden: https://de.statista.com/themen/2499/paypal/
[24] Martin Schallbruch, *Schwacher Staat im Netz*, 2018, S. 26.
[25] Bertelsmann Stiftung, *Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data*, 2017, S. 5.

über das Konsumverhalten, über soziales Verhalten und Netzwerke, Bewegungsdaten oder Gesundheits- und Fitnessdaten. Im Internet der Dinge werden zudem ständig Daten durch Geräte generiert und verarbeitet. Diese großen und komplexen Datenmengen werden oft als „Big Data" bezeichnet[26]. Das „Big" bezieht sich dabei auf die drei Dimensionen volume (Umfang der Daten), velocity (Geschwindigkeit, mit der Datenmengen generiert werden) und variety (Bandbreite der Datentypen).27

Um diese Datensets nutzbar zu machen, werden verschiedene fortgeschrittene Datenverarbeitungsmethoden (zum Beispiel predictive analytics Software, NoSQL Datenbanken, Stromanalyse-Software u.a.) eingesetzt. Dienste und Produkte können auf Grundlage der gesammelten Daten stetig personalisiert und differenziert werden. Zunehmend werden außerdem Algorithmen zur Vorhersage von bestimmtem Nutzerverhalten – ob im E-Commerce-, Gesundheits- oder Mobilitätsbereich – eingesetzt. Diese Technologien können zur Verbesserung von Angeboten für Kunden dienen. Mit Hilfe von Big Data lassen sich in kommerzieller Hinsicht Geschäftsmodelle verbessern und Wettbewerbsvorteile generieren. In unterschiedlichen Sektoren können die gesammelten Daten zusätzlich der Forschung zur Verbesserung der Lebensverhältnisse dienen. Zugleich ermöglichen sie aber ein Scoring in sozialer, finanzieller und gesundheitlicher Hinsicht – mit unabsehbaren Konsequenzen für das Individuum. So entsteht Potential für Diskriminierung und mangelnde Transparenz. Ein Individuum kann in der Regel nicht mehr nachvollziehen, wie ein Scoring-Wert und darauf basierende Entscheidungen zustande gekommen sind, geschweige denn diese anzweifeln.28

Big Data-Anwendungen, deren Ziel das Sammeln und Verarbeiten von großen Datenmengen ist, stellt Datenschutzkonzepte demnach vor erhebliche Herausforderungen. Big Data-Anwendungen und Datenschutz können deshalb im Hinblick auf personenbezogene oder personen-beziehbare Daten im Widerspruch zueinanderstehen, weil das Sammeln und Verarbeiten großer Datenmengen mit bestimmten Grundsätzen der DSGVO nur schwer in Einklang zu bringen sind.

Die Erhebung von großen Datenmengen steht grundsätzlich in einem Spannungsverhältnis zum datenschutzrechtlichen Grundsatz der Datensparsamkeit aus Art. 5 DSGVO.29 Die Zweckbindung aus Art. 5 DSGVO legt zudem fest, dass personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben und nur für diese Zwecke weiterverarbeitet werden dürfen. Dies kollidiert mit dem Sammeln von Daten ohne konkreten Anlass, wie es bei manchen Big Data-Anwendungen geschieht. Denn oft werden diese Daten gerade ohne einen bestimmten Anlass gesammelt, um neue Informationen zu generieren und die Daten später für anfänglich noch nicht bestimmbare sekundäre Zwecke einzusetzen. Ein nicht nachvollziehbares Sammeln von Daten kann überdies dem Transparenz-Gebot aus Art. 5 DSGVO entgegenstehen.

Trotz dieser Spannungsverhältnisse sind Big Data-Anwendungen grundsätzlich auch auf Basis der DSGVO möglich. Die DSGVO hat jedoch einen sehr risikobewussten Ansatz gewählt und hält an einem Verbot mit Erlaubnisvorbehalt fest. Danach dürfen personenbezogene Daten nur erhoben und verarbeitet werden, wenn der Inhaber der Daten seine Einwilligung nach Art. 6 DSGVO erteilt hat oder ein anderer Erlaubnistatbestand einschlägig ist. Das Einholen von Einwilligungen erweist sich jedoch häufig wegen des Aufwandes als praktisch schwierig oder verkommt zur Formsache, die im Angesicht der Komplexität und Länge vieler Datenschutzerklärungen und allgemeiner Geschäftsbedingungen für Betroffenen kaum wahrnehmbar ist.30

26 Vgl. https://wirtschaftslexikon.gabler.de/definition/big-data-54101/version-277155
27 Gandomi, A. und Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, 35(2).
28 Schwerk, A.; Thoms, J.; Rabl, T.; Markl, V. (2018). Datensouveränität: Fortschritt und Verantwortung (Preprint).
29 Vgl. dazu: De Mooy, M. (2018). Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data. *Bertelsmann Stiftung & Center for Democracy and Technology*.
30 Hoffmann, J.; Bergemann, B. (2017). Die informierte Einwilligung: ein Datenschutzphantom. Abrufbar unter: https://netzpolitik.org/2017/die-informierte-einwilligung-ein-datenschutzphantom/

Begriff der Datensouveränität

Vor dem Hintergrund dieser gesamtgesellschaftlichen Entwicklung stellt sich die Frage, wie Nutzer einen Überblick und eine Art von Kontrolle über ihre Daten erlangen und behalten können. In jüngerer Zeit ist in dem deutschen politischen Diskurs der Begriff „Datensouveränität" entstanden. Was per definitionem unter der Begrifflichkeit zu verstehen ist, ist umstritten. Einigkeit besteht weitestgehend darüber, dass der Begriff Datensouveränität nicht gleichzusetzen ist mit dem Recht auf informationelle Selbstbestimmung, wie es vom BVerfG aus Art. 1 und Art. 2 GG entwickelt hat (APR des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG BVerfGE 65,1 – Volkszählungsurteil). [31] Vielmehr wird darin in der Regel ein Instrument zur Kontrolle über die eigenen Daten zu sehen, die Fähigkeit zu selbstbestimmtem Handeln im digitalen Raum. Als Gegenthese zum restriktiven Datenschutz wird der Begriff Datensouveränität verwendet, um die Möglichkeit zu betonen, mit Daten zu arbeiten und sie als „Treibstoff" wirtschaftlichen Prozessen zuzuführen. Der Begriff Datensouveränität wird vereinzelt auch als Lobbybegriff gesehen und erhält damit eine negative Konnotation.[32] Der letztgenannten These folgend würde Datensouveränität der Datensparsamkeit und Datenminimierung diametral entgegenstehen.

Insgesamt liegt die Herausforderung der modernen Digitalwirtschaft im Hinblick auf den Umgang mit Daten vor allem darin, Transparenz sicherzustellen, Nutzern eine souveräne und informierte Nutzungsentscheidung zu ermöglichen und gleichzeitig innovations- und technologieoffen zu sein. Im Workshop bestand Einigkeit darüber, dass zur Erreichung dieser Ziele die Stärkung der IT-Standorte Deutschland und Europa sowie die Reduzierung der Abhängigkeiten von ausländischen Technologien in kritischen Bereichen notwendig sind.

2. Ergebnisse der Debatte und Schlussfolgerungen

Den Begriff der Datensouveränität mitgestalten

Die Debatte hat gezeigt, dass der Begriff der Datensouveränität als prozeduraler Begriff zu verstehen ist, wonach die Nutzer im Digitalen Raum in die Lage versetzt werden müssen, mit ihren Daten selbstbestimmt umgehen zu können. Der Begriff, der aus dem deutschen politischen Kontext heraus erwachsen ist, soll als eine Art der Stärkung der Nutzer verstanden werden, informierte Entscheidungen zu treffen. Der Gestaltungsspielraum sollte dazu genutzt werden, den Begriff mit einer positiven Konnotation zu versehen.

Neben der Datensouveränität des Einzelnen wurde auch der Aspekt der gesellschaftlichen Datensouveränität erörtert. Zentrale Frage war, inwieweit Deutschland und Europa im internationalen Kontext Standort für Datensouveränität werden können. Marktstarke internationale Digitalkonzerne haben Zugriff auf große Datensätze der Nutzer und können dadurch Wettbewerbsvorteile generieren. Diese Datensätze sind insbesondere für Anwendungen des maschinellen Lernens, einer Unterform der Künstlichen Intelligenz (KI), von entscheidender Bedeutung. Eine Datennutzung in dem Bereich der KI, einer der Schlüsseltechnologien der Digitalisierung, hat eine erhebliche volkwirtschaftliche Bedeutung für die Innovationsfähigkeit von Deutschland und Europa. Es gilt dementsprechend neben der Datensouveränität des Individuums eine gesellschaftliche Datensouveränität zu etablieren und Lösungen zu entwickeln, welche die Abhängigkeiten von großen internationalen Digitalkonzernen verringern und zugleich keine Abschottungsstrategie nach dem Beispiel Chinas verfolgen. Ansätze weiterer Regulierung wurden als nicht zielführend erachtet, da diese die Markteintrittshürden für Mitbe-

[31] Vgl. dazu https://www.heise.de/newsticker/meldung/Datensouveraenitaet-Die-Saege-am-informationellen-Selbstbestimmungsrecht-3953776.html

[32] Vgl. dazu https://www.heise.de/newsticker/meldung/Datensouveraenitaet-Die-Saege-am-informationellen-Selbstbestimmungsrecht-3953776.html

werber aufstellen, wodurch die Marktkonzentration der großen Digitalkonzerne weiteren Zuwachs erfährt.

Kompetenzen fördern, um Datensouveränität zu ermöglichen

Um eine individuelle Datensouveränität zu ermöglichen, bedarf es zuvörderst einer Kompetenzförderung durch digitale Bildung. In diesem Kontext stehen die Vermittlung von Medienkompetenz und Datenschutzkompetenz in den Schulen im Vordergrund. Neben der Entwicklung des Schul- und Hochschulsystems, bedarf es auch des Engagements der Unternehmen, Weiterbildungsangebote zur Förderung der Digitalkompetenz bereitzustellen.

Im Industriebereich sind laut einer Studie des Forschungszentrums Informatik, der Accenture GmbH und der Bitkom Research GmbH deutsche Anbieter bei Trendthemen im Bereich Hardware-Architekturen und Infrastrukturen sowie beim Einsatz skalierbarer Cloud-Technologien und -Anwendungen gut aufgestellt.[33] Jedoch fehlt den meisten deutschen Unternehmen noch eine Strategie für den Umgang mit Plattformen, was sowohl die Abhängigkeit von externen Plattformen als auch den Aufbau und die Nutzung von Plattformen für die eigenen Geschäftsmodelle umfasst. Außerdem spielen deutsche Anbieter von IT-Sicherheitstechnologien trotz hoher inländischer Marktanteile international nur eine geringe Rolle. Entsprechende Geschäftsstrategien könnten den Export solcher Technologien fördern, insbesondere im europäischen Binnenmarkt. Den Einsatz von IT-Sicherheitstechnologien können deutsche und europäische Firmen nutzen, um die Datensouveränität von Nutzern zu stärken.

Möglichkeiten zur Umsetzung von Datensouveränität

Einen Lösungsansatz bieten sogenannte PIMS (Personal Information Management Services). Personal Information Management Systeme sind Systeme, die natürlichen Personen mehr Kontrolle über ihre personenbezogenen Daten geben und ihnen auf diese Weise, die Möglichkeit geben, ihre personenbezogenen Daten in sicheren, lokalen oder Online-Speichersystemen zu verwalten und sie zu teilen, wann und mit wem sie es wünschen.[34]

Ziele der PIMS sind es, dem Nutzer die Kontrolle über die eigenen Daten zu geben und Transparenz zu gewährleisten. Darüber hinaus sollen sie dabei unterstützen, die Datenschutzgrundsätze der DSGVO umzusetzen und Lösungen im Rahmen des Einwilligungsprozesses bereitstellen. PIMS können Nutzern die Möglichkeit geben, Datenschutzpräferenzen selbstbestimmt zu setzen. Je nach Anwendung können PIMS automatisierte Einwilligungsverfahren und Verfahren zur Datenübertragbarkeit abbilden.

Wie die Stiftung Datenschutz in einer Studie[35] zum Thema darstellt, können PIMS-Lösungsansätze demnach unterschiedlich breit aufgestellt sein. Einige Projekte (PGuard oder MyPermission) verfolgen das Ziel, die Nutzeraufklärung zu verbessern, indem sie Nutzern einen Einblick in ihre gespeicherten personenbezogenen Daten erhalten, wodurch sie ihr Surfverhalten anpassen können. Auch gibt es Projekte, die Nutzer für ihre Daten monetär kompensieren sollen, was den Wert der Daten verdeutlicht und ihnen zumindest einen gewissen finanziellen Ausgleich bietet.[36]

Um die Datensouveränität im Sinne der Kontrolle über die eigenen Daten mit einem breiteren Ansatz auszuüben, eignen sich umfassende Datenschutz-Management-Lösungen, welche Nutzern die Möglichkeit bieten, ihre Daten innerhalb eines PIMS Dienste-übergreifend zu verwalten.

[33] Forschungszentrum Informatik, Accenture GmbH, Bitkom Research GmbH. (2017). Kompetenzen für eine Digitale Souveränität.
[34] https://edps.europa.eu/data-protection/our-work/subjects/personal-information-management-system_de
[35] Stiftung Datenschutz. (2018). Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen.
[36] Ibid.

Plattformdebatte Digitale Bildung – November 2018

Tanja Strüve und Martin Schallbruch

Im November 2018 war das Digital Society Institute Gastgeber der Plattformdebatte Digitale Bildung, die im Rahmen eines Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen ausgerichtet wurde. Im Rahmen der Veranstaltung diskutierten die Teilnehmer darüber, welche Rolle digitale Plattformen insbesondere im Schulalltag einnehmen können, um die Chancen der Digitalisierung in diesem Bereich zu nutzen. Darüber hinaus wurden Anforderungen an handelnde Akteure, ID-Management Systeme und rechtliche Anforderungen identifiziert. Impulse zu der Debatte steuerten Dr. Anja Hagen (Education 360°), und Dr. Dirk Woywod (VERIMI GmbH) bei.

1. Sachstand

Chancen und Herausforderungen der Digitalisierung im Bereich der Bildung

Der digitale Wandel hat Auswirkungen auf alle Bildungssektoren. Er sorgt für tiefgreifende Veränderungen in der schulischen Bildung, der Hochschulbildung und im Bereich der Aus- und Weiterbildung. Der Gebrauch digitaler Medien, wie Tablets oder Smartphones, ermöglicht nahezu unbegrenzten Zugang zu Wissen. Darüber hinaus bieten digitale Bildungsangebote die Möglichkeit, die Lerninhalte und die konkrete Umsetzung der Wissensvermittlung den individuellen Bedürfnissen der Lernenden anzupassen und somit eine individuelle Förderung zu ermöglichen. Im Bereich der Hochschul- sowie der Aus- und Weiterbildung bietet die orts- und zeitunabhängige Verfügbarkeit digitaler Bildungsangebote den Lernenden große Flexibilität. Darüber hinaus eröffnen sie neue Kommunikationsmöglichkeiten unter allen Akteuren des Bildungsbereichs und ermöglichen neue Formen der Zusammenarbeit.

Nach dem Leitbild der Kultusministerkonferenz (KMK) muss Lernen im Digitalen Raum dem Primat des Pädagogischen, d.h. dem Bildungs- und Erziehungsauftrag folgen. Dementsprechend soll der digitale Wandel die bildungspolitischen Leitlinien ergänzen durch Änderungen in der Gestaltung der Lernabläufe, Selbstständigkeit der Lernenden fördern und individuelle Stärken durch digitale Lernmittel verbessern[37]. Um die Digitalisierung im schulischen Bereich zu fördern und Kindern durch pädagogische Begleitung frühzeitig Kompetenzen im digitalen Raum zu vermitteln, hat die KMK das Ziel, Schülerinnen und Schülern bis 2021 den Zugang zum Internet und zu einer digitalen Lernumgebung zu bieten[38]. Dazu sollen die Länder zum einen in den Lehr- und Bildungsplänen die Vermittlung von Kompetenzen für eine selbstbe-

[37] Kultusministerkonferenz, Bildung in der digitalen Welt-Strategie der Kultusministerkonferenz, S. 9 https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2018/Strategie_Bildung_in_der_digitalen_Welt_idF._vom_07.12.2017.pdf, abgerufen am14.01.2019

[38] Ebenda, S.11.

stimmte Teilhabe in der digitalen Welt fächerübergreifend verankern, so dass der Erwerb dieser Kompetenzen über vielfältige Lernmöglichkeiten stattfindet. Zum anderen sollen im Rahmen der curricularen Vorgaben digitale Lernumgebungen systematisch genutzt werden[39].

Zugleich gehen mit der Digitalisierung im Bildungswesen vielfältige Herausforderungen einher. Eine Grundvoraussetzung für einen Wandel im Bildungsbereich ist eine leistungsfähige Netzinfrastruktur sowie die Ausstattung der Schulen mit den entsprechenden digitalen Lernmaterialien. Um entsprechende digitale Kompetenzen vermitteln zu können, bedarf es der erforderlichen Qualifikation der Lehrenden durch eine entsprechende Aus-, Fort- und Weiterbildung. Darüber hinaus sind bei dem Einsatz digitaler Lehrmaterialen datenschutz- sowie urheberrechtliche Fragestellungen zu beachten. Eine besondere Herausforderung für die Digitalisierung des Bildungssektors stellt die föderal strukturierte Bildungslandschaft mit den vielfältigen Akteuren, den unterschiedlichen Zuständigkeiten und Schulformen dar.

Digitale Plattformen im Bildungssektor

Die Bedeutung digitaler Plattformen nimmt kontinuierlich zu. In der Regel bieten sie Nutzern unterschiedliche Informations-, Kommunikations-, Kollaborations- und Handels-Dienste an. Typischerweise basieren Plattformangebote auf der Verwaltung einer (initial verifizierten) Identität und umfassen auch Leistungen wie ein Single-Sign-On sowie Verwaltungs-, Auswertungs- und Sicherheitsfunktionen rund um die digitale Identität.

Auch im Bereich der Schul-, Aus- und Weiterbildung haben digitale Plattformen eine zunehmend bedeutsame Rolle. Kollaborative Austauschplattformen ermöglichen gemeinsames Lernen, darüber hinaus können über Plattformen digitale Lehrangebote genutzt werden, welche die individuellen Bedürfnisse der Lernenden berücksichtigen. Im Hinblick auf die Ausgestaltung von Plattformen, insbesondere in der schulischen Bildung, sind die unterschiedlichen Interessenlagen der beteiligten Akteure zu berücksichtigen. Die Nutzer der Plattformen, Schülerinnen/ Schüler sowie deren Eltern und Lehrkräfte legen Wert auf die Einhaltung datenschutzrechtlicher Bestimmungen. Darüber hinaus sind eine einfache und einheitliche Bedienbarkeit von Bedeutung sowie eine möglichst nahtlose Integration von unterschiedlichen (Dritt-)Diensten. Das Interesse der Anbieter liegt in einem diskriminierungsfreien Zugang zu den Anwendungen sowie eine möglichst große Reichweite. Das öffentliche Interesse besteht zuvörderst darin, Chancengleichheit im Bildungsbereich zu gewährleisten, den rechtlichen Anforderungen im Hinblick auf Datenschutz-, Urheber- und Vergaberecht zu entsprechen. Darüber hinaus spielen die unterschiedlichen Zuständigkeiten der Länder und der Kommunen eine virulente Rolle.

Bildungsplattformen existieren schon heute mit unterschiedlicher Funktionalität auf verschiedenen Ebenen des öffentlichen Bereichs ebenso wie als Angebote privater Marktteilnehmer. Zu den bundesweiten Plattformprojekten im Bereich der allgemeinbildenden Schulen zählt die vom Bund geförderte „Schulcloud“ des Hasso-Plattner-Instituts. Mit der Cloud-Infrastruktur der Schulcloud sollen Schüler/innen, Lehrkräfte und Eltern ort- und zeitunabhängig Zugang zu den webbasierten Lehr- und Lernmaterialien haben. Die Programme und Nutzerprofile befinden sich in einem Rechenzentrum, um Aktualisierungen von Hard- und Software, Konfigurationen und Updates kümmern sich Experten.[40] Bundeslandspezifische Projekte sind u.a. „Logineo“, die Niedersächsische Bildungscloud und „Ella“. Die nordrhein-westfälische digitale Arbeits- und Kommunikationsplattform LOGINEO NRW wurde im Oktober bereitgestellt, es wurde eine Pilotphase durchgeführt und eine Einführung für den schulischen Regelbetrieb ist für Februar 2019 geplant.[41] Die Niedersächsische Bildungsplattform (NBC), die im

[39] Ebenda, S.12
[40] Hasso-Plattner Institut: https://hpi.de/open-campus/hpi-initiativen/schul-cloud.html; abgerufen am 10.01.2019.
[41] Ministerium für Schule und Bildung des Landes Nordrhein-Westfalen: http://www.logineo.schulministerium.nrw.de/LOGINEO/Startseite/; abgerufen am 10.01.20019.

Auftrag des Niedersächsischen Kultusministeriums von der Landesinitiative „n-21 Schulen in Niedersachsen online e.V." bereitgestellt wird, steht seit dem 20. Februar 2018 derzeit 45 Projektschulen zur Erprobung zur Verfügung.

Mit Hilfe der Schulcloud werden die digitalen Lern- und Arbeitsumgebungen der einzelnen Schulen eingebunden und eine schulübergreifende Zusammenarbeit ermöglicht. Das NBC Konzept besteht aus drei Ebenen: Ebene 1 stellt eine Arbeitsplattform dar, welche die Userverwaltung durchführt und in einem kommunalen Rechenzentrum gehostet wird. Die verschiedenen Lern- und Arbeitsumgebungen auf schulische Ebene (Ebene 3) werden durch einen Vermittlungsdienst bzw. eine dokumentierte API-Schnittstelle (Ebene 2) mit der Arbeitsplattform verbunden[42]. Die Zukunft der von der grün-schwarzen Regierung in Baden-Württemberg geplante Bildungsplattform "elektronische Lehr- und Lernassistenz", kurz „Ella", ist derzeit unklar[43].

2. Ergebnisse der Debatte

Erfordernis einer übergreifenden Architektur und Umsetzungsstrategie

Die Strategie der KMK „Bildung in der digitalen Welt" ist keine ausreichende Grundlage für den Aufbau digitaler Bildungsplattformen. Insbesondere fehlt eine Zielarchitektur, wie digitale Bildungsplattformen ausgestaltet werden. Die Definition der Architektur muss auf Landesebene erfolgen und zwischen Landesregierung und Schulträgern vereinbart werden. Im Rahmen einer solchen Architektur können Fragen der Funktionalitäten von Bildungsplattformen, der Einbindung interner und externer Dienstangebote sowie der querschnittlichen Fragen (wie Interoperabilität) festgelegt werden. Hierauf aufbauend kann eine Umsetzungsstrategie erarbeitet werden, letztlich auch eine Betriebs- und Weiterentwicklungsstrategie.

Erfordernis einer digitalen Identität im Bildungssektor

Die Teilnehmer der Debatte waren sich einig, dass ein Identitäten-Management Kern einer Zielarchitektur für Bildungsplattformen sein muss. Das Identitäten-Management ist im schulischen Kontext Voraussetzung für unterschiedliche Plattform-Funktionalitäten, etwa die digitale Ablage, die Nutzung digitaler Lehrangebote (Berechtigungs- und Lizenzverwaltung), die Kooperation und Kommunikation innerhalb der Schule ebenso wie die Schulverwaltung. Während das Identitäten-Management zentral organisiert werden könnte (und sollte), müsste das Lern-Management auf die jeweiligen Schulformen und die entsprechenden Schüler angepasst werden.

Vor diesem Hintergrund entwarfen die Teilnehmer der Debatte eine architekturelle Ausgestaltung des ID-Managements. Über eine schulübergreifende Elementar-Plattform sollte das Identitäten-Management von Schülerinnen und Schülern, Eltern und Lehrkräften abgebildet werden, eine Art schulübergreifender Vermittlungsdienst. Die entsprechenden Lern-Anwendungen, welche den individuellen Bedürfnissen der jeweiligen Schulformen und ihrer Schülerinnen und Schüler entsprechen, sowie die administrativen Aufgaben könnten über interoperable standardisierte Schnittstellen mit der Basisplattform verbunden werden.

Im Teilnehmerkreis streitig war die Frage, ob bzw. inwieweit private Anbieter ein Identitäten-Management für die staatliche Schulbildung bereitstellen können und sollten oder ob das übergreifende Identitäten-Management eine öffentlich zu organisierende Aufgabe ist. Einvernehmen

[42] NIEDERSÄCHSISCHE BILDUNGSCLOUD – Landesinitiative n-21 Schulen in Niedersachsen online e.V.: https://www.niedersachsen.cloud/; abgerufen am 10.01.2019.

[43] SWP: https://www.swp.de/impressum/; abgerufen am 10.01.2019.

bestand über den öffentlichen Charakter dieser Aufgabe, so dass die Schulverwaltung mindestens eine Gewährleistungsverantwortung für das Identitäten-Management hat.

Erforderlichkeit von Medienkompetenz der Lehrenden

Der aktive Einsatz digitaler Bildungsmedien setzt eine entsprechende Qualifikation der Lehrkräfte voraus. Derzeit sind viele in der Anwendung medialer Technik nicht ausreichend geschult, weshalb sie die bereits vorhandenen digitalen Angebote nur unzureichend nutzen. Entsprechende Kompetenzen müssen in Aus- und Weiterbildung der Lehrkräfte vermehrt vermittelt werden. Zielführend kann sein, die erforderlichen Fortbildungen im Bereich Digitalkompetenzen in der Arbeitszeit der Lehrkräfte abzubilden.

Rechtliche Rahmenbedingungen

Eine entscheidende Rolle bei der Verwendung digitaler Plattformen im Bildungsbereich kommt den rechtlichen Rahmenbedingungen, hier vor allem auch dem Datenschutz, zu. Bei der Nutzung von Online-Lernplattformen zur Aufgabenbearbeitung, für Lernkontrollen, oder für Gruppenarbeiten fallen personenbezogene Daten an, welche dem Anwendungsbereich der Datenschutzgrundverordnung unterfallen. Eine rechtmäßige Verarbeitung personenbezogener Daten bedarf einer der in Artikel 6 DSGVO normierten Erlaubnistatbestände. Im Hinblick auf den Einsatz von Lernplattformen kommt der Erlaubnistatbestand nach Art. 6 Abs. 1 lit e in Verbindung mit Art. 6 Abs. 3 S.1 lit b DSGVO mit den jeweiligen Schulgesetzen bzw. Schuldatenschutzgesetzen in Betracht. In diesem Zusammenhang ist zu prüfen, ob die erhobenen Daten für eine Aufgabenwahrnehmung im schulischen Kontext erforderlich sind. Sofern dies nicht der Fall ist, kommt allein eine Einwilligung nach Art. 6 Abs. 1 lit a DSGVO in Betracht, wobei die besonderen Bedingungen für die Einwilligung eines Kindes gemäß Art. 8 DSGVO Beachtung finden müssen. Danach kann das Kind die Einwilligung selbst erteilen, sofern es das 16. Lebensjahr vollendet hat, andernfalls bedarf es der Einwilligung durch den Träger der elterlichen Sorge. Darüber hinaus sind von den Anbietern von ID-Diensten oder Lernplattformen nach Art. 25 DSGVO technisch-organisatorische Maßnahmen zu ergreifen, um Datenschutzgrundsätzen wie der Datensparsamkeit zu entsprechen.

Eine weitere datenschutzrechtliche Problematik liegt in der Auftragsverarbeitung. Nutzen Schülerinnen und Schüler interaktive virtuelle Bildungsmedien, die individuell konfigurierbar sind oder den individuellen Lernfortschritt speichern, ist der Betreiber des Bildungsmedium Auftragsdatenverarbeiter. Um den Anforderungen der DSGVO zu entsprechen, schließen derzeit im Extremfall alle 40.000 Schulen Verträge zur Auftragsverarbeitung mit den Bildungsanbietern ab, um die Daten datenschutzkonform bei einem Anbieter zu verarbeiten. Sofern die rechtlichen Rahmenbedingungen entsprechend geschaffen würden, könnte das Verfahren vereinfacht werden, indem sich die Anbieter von digitalen Medien zertifizieren lassen, so dass Schulen leichter datenschutzrechtliche Überprüfungspflichten erfüllen können. Hierdurch könnte erreicht werden, dass insbesondere Überprüfungspflichten der Schulen als Verantwortlicher der Verarbeitung der Daten bei den Anbietern vereinfacht werden könnten.

Auch urheberrechtliche Fragestellungen sind im Hinblick auf den Einsatz digitaler Plattformen und das Einstellen von Lehrmaterialen durch Lehrer und Schüler von Bedeutung. Urheberrechtliche Schrankenregelungen ermöglichen die Nutzung von Werken ohne die Einwilligung des Rechtsinhabers und beschränken auf diese Weise das ausschließliche Recht des Urhebers. Diese Ausnahmen wurden u.a. für den Bereich Bildung im UrhWissG neu geregelt, um die Nutzung im digitalen Raum zu ermöglichen. Die Schrankenregelung des § 60a UrhG erlaubt es, für den Unterricht und die Lehre an Bildungseinrichtungen (z.B. Schulen und Hochschulen) grundsätzlich bis zu 15 Prozent eines Werkes zu nutzen. Nach der Regelung des § 60 b UrhG wird die Herstellung von Unterrichts- und Lehrmaterialen erleichtert. Diese Regelungen ersetzen indes nicht die Lizenzangebote der Verlage, so dass diese auch in Zukunft eine tragende Rolle im Bereich der Bildung haben werden.

Um digitale Lehrangebote über digitale Plattformen nutzen zu können, ist die faktische Teilhabemöglichkeit aller Schülerinnen und Schüler zu gewährleisten, damit die Schule als staatliche Institution dem Gleichbehandlungsgrundsatz aus Art. 3 Grundgesetz nachkommt.

Standardisierte Schnittstellen und Interoperabilität

Plattformen im Bildungsbereich sollten schon wegen der Vielfalt der Funktionalitäten und miteinander interagierenden Dienste zwingend offen und interoperabel ausgestaltet sein. Durch die Implementierung solcher Schnittstellen, könnte ein Identitäten- Management im Bildungssektor leichter umgesetzt werden, welches zugleich für alle Akteure des Bildungswesens nutzbar wäre.

Plattformdebatte Smart Home – Januar 2019

Martin Schallbruch, Isabel Skierka, Tanja Strüve und Alexander Gerberich

Im Januar 2019 war das Digital Society Institute Gastgeber der Plattformdebatte Smart Home, die im Rahmen eines Begleitforschungsprojektes zur gesellschaftlichen Verankerung digitaler Plattformen ausgerichtet wurde. Im Rahmen der Veranstaltung diskutierten die Teilnehmer darüber, welche Rolle digitalen Plattformen im Bereich Smart Home zukommt. Darüber hinaus adressierten die Teilnehmer die Smart-Home-spezifischen Risiken für Datenschutz und Datensicherheit.
Impulsvorträge zu der Debatte trugen Bernd Kowalski (Bundesamt für Sicherheit in der Informationstechnik), Michael Schidlack (Wirtschaftsinitiative Smart Living), Günther Ohland (Smart Home Initiative Deutschland e.V.) und Benjamin Spoden (Verimi GmbH) bei.

1. Sachstand

Smart Home- Verbreitung

Sprachassistenten, ‚intelligente' Thermostate, smarte Fernseher, Glühbirnen, Türschlösser, Kühlschränke, Waschmaschinen oder andere Geräte finden sich immer häufiger im Zuhause vieler Menschen. Nicht zuletzt durch die Popularität von Amazon Alexa oder Google Home verbreitet sich das „Smart Home" in vielen Haushalten. „Smart" bedeutet in diesem Kontext die Vernetzung von Geräten untereinander, um auf diese Weise Prozesse überwachen, steuern oder automatisieren zu können.

In einem Smart Home werden Geräte der Hausautomation (z.B. Beleuchtung, Heizung), Haushaltstechnik (Kühlschrank, Waschmaschine, etc.), Konsumelektronik (z.B. Fernseher) und Kommunikationseinrichtungen (z.B. Telefonanlagen) zu intelligent interagierenden Gegenständen, die sich an den Bedürfnissen der Bewohner orientieren.[44] Die Vernetzung der Gegenstände bringt Assistenzfunktionen und Dienste mit sich, die zu einem Mehrwert für Nutzer führt.

Die Gründe für die Nutzung von Smart Home Anwendungen sind u.a. zusätzlicher Komfort, Sicherheit, Senkung der Heiz- und Stromkosten, Schutz der Umwelt sowie zusätzliche Entertainmentmöglichkeiten.[45] Nach einer Prognose von Deloitte wird es 2020 nach einem konservativen Szenario eine Million Smart-Home-Haushalte geben, nach einem progressiven Szenario werden es 1,45 Millionen sein.[46] Experten rechnen ab 2020 mit einem Durchbruch von Smart Living zum Massenmarkt.[47]

Ein Smart Home besteht dabei im Wesentlichen aus drei Komponenten: den Sensoren wie Thermometer, Bewegungsmelder oder Überwa-

[44] VDI/VDE, Smart Home in Deutschland; Untersuchung im Rahmen der wissenschaftlichen Begleitung zum Programm Next Generation Media (NGM) des Bundesministeriums für Wirtschaft und Technologie, Hartmut Strese, Uwe Seidel, Thorsten Knape, Alfons Botthof, S. 8
[45] Deloitte Smart Home Consumer Survey 2018, S.18

[47] GlobalSmartHomeExpertsMonitor,2018,KOTSCHICONSULTING

chungskameras, den Aktoren wie Heizungsthermostat oder Lampe und einer Steuereinheit, die mit dem Internetrouter verbunden ist, wobei mittlerweile die meisten Geräte Aktoren und Sensoren gleichzeitig sind. Dem Router kommt im Smart Home eine entscheidende Rolle zu, da er den Zugang zum Internet darstellt und über ihn die Daten und Informationen laufen.

Herausforderungen Interoperabilität, Datenschutz und Datensicherheit

Eine Kernherausforderung für die Nutzung von Smart-Home-Anwendungen ist die Interoperabilität von Systemen. Diese bezeichnet die Fähigkeit, Daten fehlerfrei auszutauschen und Informationen und Befehle korrekt zu verstehen, zu interpretieren und umzusetzen.

Grundvoraussetzung für Interoperabilität auf der technischen Ebene sind gemeinsame Schnittstellen und gemeinsame Standards. Offene Standards sind dabei in der Regel besonders Interoperabilitäts-fördernd. Doch die meisten Smart-Home-Systeme und Anwendungen verwenden unterschiedliche Standards und Protokolle. Das gilt sowohl für die Kommunikation zwischen Geräten sowie für die Software auf Anwendungsebene.

Auf der Ebene der Kommunikationsprotokolle existieren eine Vielzahl unterschiedlicher Protokolle, über die sich smarte Produkte verbinden lassen. Dieses sind beispielsweis Wi-Fi Direct, Bluetooth Smart, ZigBee, Z-Wave und HomeMatic.

Die Implementierung unterschiedlicher Protokoll-Schnittstellen und Standards führt zu einer Segmentierung und Inkompatibilität von Smart-Home-Angeboten. Die fehlende Interoperabilität von Anwendungen und Systemen wiederum erschwert Nutzern die Bedienung und Implementierung von Smart-Home-Lösungen, was die Nutzung insgesamt hemmt. Obwohl sogenannte ‚Hubs' eine Integration verschiedener Smart-Home-Anwendungen mit unterschiedlichen Kommunikationsprotokollen und Anwendungssoftware ermöglichen, müssen Nutzer meist mehrere Systeme parallel bedienen und verwalten.

Die Vernetzung des eigenen Zuhauses wirft zahlreiche rechtliche Fragen auf, insbesondere im Hinblick auf den Datenschutz. Von besonderer Relevanz ist dabei, welche Daten von den smarten Haushaltsgeräten erfasst und an die Hersteller der Geräte bzw. an Dritte weitergegeben werden. Soweit die erhobenen Daten einen Personenbezug aufweisen, d.h. z.B. Daten des Nutzers der Smart-Home-Anwendung verarbeitet werden, sind durch den Verantwortlichen, also in der Regel den Betreiber der Anwendung (der Nutzer selbst oder auch der Vermieter) oder auch den Betreiber des zugehörigen Clouddienstes, die Vorgaben der DSGVO einzuhalten. Da die meisten SmartHome-Geräte mit dem Internet kommunizieren und schon eine dynamische IP-Adresse einen Personenbezug aufweist[48], ergibt sich nahezu immer eine Verpflichtung zur Beachtung datenschutzrechtlicher Vorschriften.

Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten durch den Verantwortlichen bei der Nutzung von Smart-Home-Anwendungen wird in der Regel die Einwilligung des Nutzers gemäß Art. 6 Abs. 1 lit. a) DSGVO sein. Hieraus folgt, dass die Einwilligung zunächst wirksam eingeholt werden muss. Dabei wird die Umsetzung der erforderlichen Transparenz und damit die Nachvollziehbarkeit der Verarbeitung der Daten eine besondere Rolle zukommen. Soweit der Nutzer seine Einwilligung widerruft, entfällt die Rechtsgrundlage für die Verarbeitung der Daten, so dass die erhobenen personenbezogenen Daten gelöscht oder zumindest anonymisiert werden müssen.

Eine weitere Herausforderung für Smart-Home Systeme ist die IT-Sicherheit. Der Smart Home Sektor ist einer der am schnellsten wachsenden Bereiche im „Internet der Dinge" (IoT). Ausweislich des Sicherheitsindex 2018 von ‚Deutschland sicher im Netz' ist trotz steigender Nutzungszahlen ein leichter Rückgang der Angriffe auf Smart Home zu verzeichnen. Danach ist die Anzahl der Angriffe auf die Hausvernetzung um 0,4 Prozent gesunken; damit waren 2,6 Prozent der Verbraucher weniger Ziel eines Angriffs.[49]

Gleichzeitig zeigt der Index, dass trotz geringer Angriffe die Verunsicherung bei Verbrauchern

[48] BGH, Beschl. v. 28.10.2014 – VI ZR 135/13; EuGH, Urt. V. 19.10.2016 – C-582/14

[49] DsiN Sicherheitsindex 2018 – Digitale Sicherheitslage der Verbraucher in Deutschland, Hrsg. Deutschland sicher im Netz, S. 34

im Hinblick auf die Nutzung von Smart Home Anwendungen im Vergleich zum Vorjahr gestiegen ist: während 2017 28,2 Prozent der Befragten die Steuerung und Vernetzung von Haustechnik für gefährlich oder sehr gefährlich hielten, waren es 2018 31,1 Prozent.[50]

Derzeit existiert keine besondere Verpflichtung zur IT-Sicherheit im Smart Home. Hersteller sind bisher an keine ausdrücklichen gesetzlichen Vorschriften oder Standards für IT-Sicherheit von Geräten im IoT gebunden. Das hat zur Folge, dass Funktionalität und Kosteneffizienz meist höhere Priorität haben als die Sicherheit von Produkten und Diensten. Daher sind viele Geräte auf dem Markt, deren Zugang gar nicht oder nur schwach, wie es bei der Nutzung von Standardpasswörtern der Fall ist, gesichert sind und damit leicht ausnutzbare Schwachstellen aufweisen. Diese ermöglicht es Hackern, Angriffe leicht und effektiv zu skalieren. Ein bekanntes Beispiel dafür ist die Mirai-Schadsoftware, welche Hacker für den Zusammenschluss von großen, teilweise aus Heim-Überwachungskameras und Babyphones bestehende Botnetze nutzten und darüber Distributed-Denial-of-Service (DDoS) Angriffe ausübten. Diese Angriffe erreichten teilweise eine Stärke von über 1 TB/s und legten zeitweise den Provider DynDNS lahm.[51]

Mangelnder IT-Sicherheit kann außerdem eine Gefahr für die Sicherheit der persönlichen Daten von Smart Home-Nutzern sowie für deren IT-Systeme darstellen. Eine Schwachstelle in einem Gerät oder gar einem Router kann als Einfallstor für Angriffe auf weitere IT-Systeme in der Wohnung werden. Darüber hinaus können Software-Schwachstellen zu einer Gefahr werden, wenn beispielsweise die Manipulation eines IT-Systems eines elektronischen Haushaltsgeräts zu einer Fehlfunktion führt oder die Schließanlage manipuliert wird und auf diese Weise Einbrechern ein Eindringen in die Wohnung ermöglicht wird.

Digitale Plattformen im Bereich Smart Home

Durch die Vernetzung von unterschiedlichen Geräten mit eigener Software von unterschiedlichen Anbietern sowie unterschiedlichen Protokoll-Schnittstellen ist das Smart Home sehr komplex.

Smart Home Hubs oder Plattformen machen diese Komplexität für den Nutzer beherrschbarer. Sie ermöglichen die ortsunabhängige Steuerung unterschiedlicher Geräte und Funktionen im Haushalt per Smartphone, Tablet oder PC. Da Hubs oder Plattformen meist unterschiedliche Protokolle unterstützen und Schnittstellen für unterschiedliche Software bereitstellen, können sie sämtliche Endgeräte vernetzen, die aufeinander abgestimmte, von Zeiten oder Anwesenheit abhängige, Aktionen ermöglichen. Über Plattformen ist auch die Einrichtung von sogenannten „Wenn-Dann-Aktionen“ („If-This-Then-That“ IFTT) möglich, die die von einem Gerät aufgenommenen Informationen in die Aktion eines anderen Gerätes umsetzen können.

Diese Plattformangebote basieren meist auf der Verwaltung einer digitalen Identität zur Steuerung verschiedener Geräte.

Amerikanische Anbieter wie Google und Amazon haben mit ihren Sprachassistenz-Systemen bereits eine führende Marktposition in diesem Bereich etabliert. Die Systeme sind kompatibel mit einer Vielzahl von Endgeräten und Smart Home-Plattformen. Die Anbindung an diese Systeme bietet einen Mehrwert für Anbieter von Smart Home-Lösungen, so dass Hersteller weltweit selbst die Kosten und den Aufwand für die Kompatibilität ihrer Geräte und Systeme mit Google und Amazon übernehmen.

Auch Apple hat 2014 mit dem HomeKit eine Smart Home-Plattform auf den Markt gebracht, die die Steuerung verbundener Geräte mit einem Smartphone bzw. Tablet und die Automatisierung einiger Aktionen im Haushalt möglich macht. Eine sprachliche Steuerung ist mit der Spracherkennungssoftware „Siri“ möglich. Die Anmeldung und Steuerung beim HomeKit erfolgten auf jedem Gerät mithilfe der Apple-ID über die iCloud. Innerhalb der iCloud sind alle genutzten Endgeräte miteinander verbunden.

Unter den deutschen Plattform-Anbietern ist die QIVICON-Plattform der Deutschen Telekom führend. Über QIVICON lassen sich verschiedene

[50] ebd.

[51] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

Smart-Home Endgeräte mit eigener Software steuern. Die Plattform hat Schnittstellen mit verschiedenen Funkstandards, was eine Komptabilität mit Diensten verschiedener Anbieter erlaubt. Über Sprachassistenten wie Amazons Alexa oder Google Home Sprachassistenten ist außerdem eine Sprachsteuerung möglich.

2. Ergebnisse der Debatte

Interoperabilität von Geräten, Systemen und Plattformen schaffen

Erfolgreiche und breit nutzbare Smart Home-Lösungen müssen zu einem hohen Grad interoperabel sein, also über gemeinsame Schnittstellen und Standards mit anderen Lösungen Informationen austauschen können. Im Smart Home-Bereich gilt dies für die Kommunikationsprotokoll-Ebene sowie für die Anwendungs-Ebene, auf der Daten übergreifend verarbeitet und ausgewertet werden können.

Um den Datenaustausch zwischen Geräten und Anwendungen interoperabel zu gestalten, muss die Kommunikation für alle involvierten Komponenten verständlich sein und sich mit allen Vernetzungsstandards nutzen lassen.[52]

Idealerweise kann diese Interoperabilität durch einen einheitlichen Kommunikationsstandard gewährleistet werden. Zwar gibt es einige Initiativen in diese Richtung (siehe das Kommunikationsprotokoll EEBUS, welches hauptsächlich als Plattform im Energiesektor und im Bereich Smart Grid genutzt wird [53]). Die Etablierung eines einheitlichen Standards ist auf absehbare Zeit jedoch nicht realistisch. Ein wahrscheinlicheres Szenario ist eine hybride Netzwerkarchitektur, in dem Wi-Fi mit stromsparenden Wireless-Protokollen kombiniert wird. Dabei müssen zum einen die Internetverbindung zum Haushalt und die Geräteverbindung zum Netzwerk gewährleistet werden.

Über die Kompatibilität von Kommunikationsprotokollen hinaus ist ebenfalls entscheidend, dass heterogene Systeme relevante Daten geräteübergreifend nutzen, auswerten und verarbeiten können, um Entscheidungen und Ausführungen im Smart Home zu automatisieren. Meist verwenden Nutzer noch einzelne Apps zur Verwaltung von Smart Home-Funktionen. Um Apps übergreifend zu steuern, können Nutzer zurzeit auf IFTTT-Systeme zugreifen, die sie jedoch selbst stückweise konfigurieren müssen.

Da einheitliche Standards zumindest kurzfristig auf diesen Ebenen nicht realistisch sind, werden Interoperabilitätsprobleme mit Hilfe von intermediären Diensten bzw. Plattformen umgangen, welche Kommunikation und Interaktion zwischen heterogenen Systemen ermöglichen können. Durch die Kombination von verschiedenen Kommunikationsstandards wie Wi-Fi-, Zigbee-, Z-Wave-, RF- und Infrarot-Technologien lassen sich die meisten Smart Home Geräte entweder über eine direkte Schnittstelle oder über application programming interfaces (APIs) integrieren.

Digitale Smart Home-Plattformen, die Geräte, die Infrastruktur des Hauses und die Cloud-basierten Anwendungen unterschiedlicher Anbieter miteinander auf allen Ebenen ganzheitlich verbinden, haben Smart Home Hubs mittlerweile abgelöst. Die unter europäischen Anwendern erfolgreichen digitalen Plattformen in diesem Bereich werden jedoch von US-amerikanischen Firmen betrieben.

Zu beobachten ist, dass Sprachassistenzsysteme großer Anbieter wie Google, Amazon und Apple in diesem Bereich den Markt erobern. Gründe dafür sind erstens die vergleichsweisen geringen Kosten dieser Systeme für die Endnutzer, zweitens die Kompatibilität mit verschiedensten Anwendungen. Anders als Startups oder kleinere Unternehmen in diesem Bereich verfügen große Tech-Konzerne bereits über eine Marktstellung, die es ihnen erlaubt, selbst universelle Standards zu setzen. Als Folge davon bemühen sich andere Hersteller, eine Schnittstelle zu diesen verbreiteten Systemen anzubieten. Zudem verfügen diese

[52] https://www.homeandsmart.de/interoperabilitaet-im-smart-home; https://www.digitalengineering247.com/article/smart-homes-pursuit-of-interoperability/

[53] https://www.homeandsmart.de/eebus-initiative-smart-home-internet-of-things

Konzerne über die Ressourcen, um eine hohe Funktionalität und Nutzbarkeit zu gewährleisten.

Datenschutz und Datensicherheit

Die Teilnehmer waren sich darüber einig, dass dem Datenschutz im Smart Home-Bereich eine entscheidende Rolle zukommt. Im Teilnehmerkreis wurde diesbezüglich auch der Datenschutz der Hausbewohner untereinander thematisiert. In der juristischen Kommentarliteratur wird dazu ausgeführt, dass Smart Home-Anwendungen hinsichtlich der Hausbewohner untereinander nicht in den Anwendungsbereich der DSGVO fallen.[54] Demgegenüber unterfallen die Anbieter entsprechender Services, soweit diese personenbezogenen Daten der Hausbewohner verarbeiten, in den Anwendungsbereich der DSGVO.55

Hinsichtlich der Datensicherheit wurde im Rahmen der Veranstaltung festgehalten, dass die IT-Sicherheit dem Technologiefortschritt nicht standhält. Die Sicherheitsprobleme und Sicherheitsvorfälle werden sich daher zukünftig noch verschärfen. Dementsprechend bestand Einigkeit darüber, dass IT-Sicherheit ein integraler Bestandteil von IoT-Produkten sein muss. Durch Security by Design sollen die Sicherheitsanforderungen, die an Soft- und Hardware zu stellen sind, bereits in der Entwicklungsphase des Produktes Berücksichtigung finden mit dem Ziel der Sabotagefestigkeit bzw. resilienten Sicherheit. Die entsprechenden Sicherheitsstandards müssen verbindlich und – je nach Produktkategorie – verpflichtend für Hersteller sein. Smart Home-Produkte sollten demnach auf Basis bestimmter Sicherheitsstandards gekennzeichnet werden und ggf. von einer neutralen Stelle auf ihre Sicherheit hin zertifiziert sein. Sicherheits-Mindestanforderungen ließen sich beispielsweise in die CE-Zertifizierungsprozesse unter dem EU New Legislative Framework oder innerhalb der geplanten IT-Sicherheits-Zertifizierungsschemata des 2019 verabschiedeten EU Rechtsakts für die Cybersicherheit integrieren.

Eine wichtige Rolle bei der IT-Sicherheit im Smart Home kommt dem Router zu. Der Router bildet die Schnittstelle zwischen dem Internet und den privaten Netzwerken der Verbraucher und kann im ungünstigen Fall als Schwachstelle für Hackerangriffe genutzt werden und auf diese Weise Ausgangspunkt für Cyberattacken sein. Die Technische Richtlinie „Secure Broadband Router“ (TR-03148) des BSI bietet hier eine Hilfestellung auch für Verbraucher.[56]

Eine skalierbare Lösung für die IT-Sicherheit in Smart Home Produkte bietet die Implementierung von secure elements in IoT-Produkten. Relevant ist hier das OPTIMOS 2.0-Projekt, welches eine mobile Authentisierungslösung auf eIDAS-Vertrauensniveau ‚substanziell‘ anstrebt.

Erfordernis eines Identitäten-Managements im Bereich Smart Home

Die Teilnehmer der Debatte waren sich einig, dass ein übergreifendes Identitäten-Management eine Grundvoraussetzung für erfolgreiche Smart Home-Lösungen ist. Für einen hohen Nutzwert sollten digitale Identitäten einen diskriminierungsfreien Zugang zu Smart Home-Diensten und universelle Anwendbarkeit ermöglichen. Dazu bedarf es interoperablen Identitäts-Lösungen, die auf einheitlichen Protokollen und offenen Schnittstellen basieren.

Momentan sind digitale Identitäten im Smart Home-Bereich meist an einzelne Anbieter gekoppelt und daher fragmentiert. Google, Amazon und Apple ermöglichen Usern eine Anbieter-übergreifende Lösung zur Nutzung von Smart Home-Diensten über die diensteigene Identität, also Google ID, Amazon ID bzw. Apple ID. Jedoch sind diese Identitäts-Lösungen aufgrund von Tracking (außer der Apple ID) weniger vertrauenswürdig. Da Anbieter über die übergreifende Identität Nutzerdaten sammeln, verarbeiten und auswerten, können diese ID-Lösungen Risiken im Hinblick auf den Datenschutz schaffen.

Daher ist eine Kern-Anforderung an ein Identitäten-Management im Smart Home, dass dieses vertrauenswürdig ist und dass Nutzer ihre Identität komfortabel und selbstbestimmt verwalten können. Darüber hinaus sollte ein Identitäten-Management auch die Möglichkeit für ein differenziertes Rollen- und Berechtigungsmanagement im

[54] Plath in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 2 DSGVO
[55] ebd.

[56] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=2

Smart Home bieten. So sollten auch unterschiedliche Nutzer eines Wohnbereichs, z.B. Partner oder Familienmitglieder, ihre Identitäten und Daten unabhängig verwalten und die Sichtbarkeit und Privatsphäre ihrer Daten selbst bestimmen können.

Ein Identitäten-Management sollte auch eine Differenzierung zwischen unterschiedlichen Identitäts-Attributen von Nutzern ermöglich. Bei sicherheitsrelevanten Anwendungen, wie z.B. remote Zugriff auf Kameras, sollte eine sichere Zwei-Faktor-Authentisierung genutzt werden.

Digitale Identitäten im Gesundheitswesen Januar 2020

Martin Schallbruch, Tanja Strüve und Isabel Skierka

Am 28. Januar 2020 war das Digital Society Institute (DSI) der ESMT Gastgeber des Dialogformates Digitale Identitäten im Gesundheitswesen, welches im Rahmen eines von Verimi unterstützten Begleitforschungsprojekts des DSI ausgerichtet wurde. Die Veranstaltung ging der Frage nach, welche Anforderungen an digitale Identitäten im Gesundheitswesen zu stellen sind, insbesondere im Hinblick auf die Datensouveränität der Patientinnen und Patienten. Darüber hinaus diskutierten die Teilnehmerinnen und Teilnehmer des Workshops darüber, welche Besonderheiten des Gesundheitswesens im Vergleich zu anderen Sektoren zu berücksichtigen sind und welche Anforderungen darüber hinaus an sektorübergreifende Interoperabilität zu stellen sind.

Impulsvorträge zu der Debatte trugen Dr. Markus Leyck Dieken (gematik GmbH), Ralf Degner (Techniker Krankenkasse), Dr. Dina Truxius (Bundesamt für Sicherheit in der Informationstechnik) sowie Dr. Dirk Woywod (Verimi GmbH) bei.

1. Sachstand

Digitale Identitäten- Status Quo

Digitale Identitäten sind conditio-sine-qua-non einer erfolgreichen Digitalisierung der unterschiedlichen Lebensbereiche. Die Anforderungen an initiale Identifizierung und spätere Authentifizierungen variieren dabei je nach Anwendungskontext. Während im Kontext von Online-Shopping Benutzername und Passwort weiterhin die Regel darstellen, werden im öffentlichen Sektor mit der eIDAS-Verordnung oder im Zahlungsverkehrssektor mit der PSD II spezifische höhere Anforderungen zugrunde gelegt.

Ein wesentlicher Erfolgsfaktor für die Nutzung digitaler Identitäten ist eine hohe Benutzerfreundlichkeit, d.h. sie muss intuitiv bedienbar sein, eine weite Verbreitung haben und darüber hinaus transparent sein.

Einheitliche benutzerfreundliche digitale Identitätslösungen bieten amerikanische Plattformen wie Google, Apple und Facebook. Immer mehr Menschen nutzen diese Leistungen und übermitteln damit gleichzeitig persönliche Daten, welche die Digitalkonzerne zum Zwecke einer konsumentenorientierten Werbung einsetzen.

Digitalisierung im Gesundheitswesen

Digitale Technologien und Anwendungen bringen einen großen Mehrwert für die medizinische Versorgung und finden einen immer größeren Einzug in den Alltag der Menschen. Bei 1005 vom Bitkom befragten Personen stimmten 46 % der Aussage zu, dass ein Teil der medizinischen Versorgung zukünftig ausschließlich digital stattfinden muss, um den steigenden Kosten entgegen zu wirken.[57] Die elektronische Patientenakte (ePA), welche alle Patienten ab 2021 von ihren Krankenkassen erhalten sollen, ermöglicht die digitale Erfassung, Einsicht und Verwaltung von Patientendaten für Leistungserbringer und Patienten selbst. 65 % der vom Bitkom Befragten wollen die ePA nutzen.[58] Auch die meisten Medizingeräte, von Insulinpumpen

[57] Digital Health, Mai 2019 - Bitkom Research https://www.bitkom.org/sites/default/files/2019-05/190508_bitkom-pressekonferenz_e-health_prasentation.pdf

[58] Ebd.

über MRTs bis Fitness-„Wearables“ sind vernetzt und setzen fortgeschrittene Cloud-basierte Software ein. Zudem dienen Software-basierte Empfehlungen im Gesundheitsbereich zunehmend als Unterstützung für Entscheidungen im ärztlichen Arbeitsalltag. Aufgrund der besonderen Sensibilität von Gesundheitsdaten stehen neben den Chancen auch Fragen von Datenschutz und Datensicherheit, im Fokus der Diskussion. Gesundheitsdaten sind lukrativ – ob für große Technologie-Konzerne, welche diese monetarisieren oder eigene Geschäftsmodelle ausbauen möchten, für Versicherungen, aber auch für Kriminelle. Immer wieder kommt es zu Sicherheitsvorfällen, durch die Patientendaten für kriminelle Zwecke missbraucht werden. Angriffe auf oft nur schlecht gesicherte vernetzte Medizinprodukte können nicht nur den Datenschutz, sondern auch die physische Sicherheit von Patienten gefährden.

Digitale Identitäten im Gesundheitswesen

Digitale Identitäten spielen eine zentrale Rolle in der digitalen Gesundheitsversorgung. Sie sind Voraussetzung für die Nutzung der elektronischen Patientenakte (ePA), von Gesundheits- und Fitness-Apps, Medizingeräten für Patienten sowie den Zugang zu Patienten- und Versorgungsdaten und die digitale Gesundheitsinfrastruktur für Leistungserbringer. Aufgrund des besonderen Schutzbedarfs von Gesundheitsdaten müssen digitale Identitäten in diesem Bereich hohe Sicherheitsanforderungen erfüllen. Gleichzeitig müssen sie jedoch auch einfach nutzbar sein. Derzeit arbeiten Krankenkassen und andere Akteure im Gesundheitswesen an eigenen digitalen Identifizierungslösungen. Gleichzeitig expandieren jedoch auch die Digitalkonzerne Google, Apple, Facebook und Apple (GAFAs) im Gesundheitsbereich. Diese nutzen jeweils eigene übergreifende Identifizierungs- und Login-Dienste. Die Stärken der GAFA-Dienste liegen in deren hoher Usability und dem Netzwerkeffekt bzw. der Interoperabilität mit anderen Applikationen. Apple beispielsweise bietet eine eigene Gesundheitsakte an, die direkt über iOS mit der Apple-ID zugänglich ist. Apple Health bietet Schnittstellen für andere Apps, welche eine direkte Integration mit Apples Dienst ermöglichen. Ein Beispiel ist die in Deutschland gegründete erfolgreiche App „Clue“. Europäische und deutsche Anbieter von digitalen Gesundheitsangeboten und digitalen Identitäten im Gesundheitsbereich konkurrieren bereits jetzt in vielen Bereichen mit den Angeboten der GAFAs.

Übergreifende Lösungen für Identifizierungen und Authentifizierungen im Gesundheitswesen existieren in Deutschland und Europa bisher nicht. Ein wichtiger Grund dafür sind die besonderen regulatorischen Anforderungen an den Datenschutz und die Datensicherheit im Gesundheitsbereich, welche auch digitale Identitäten betreffen.

Die Anforderungen an Identitäten variieren je nach konkretem Anwendungsfall. Für den Zugriff auf Daten der elektronischen Patientenakte bedarf es gemäß § 291a SGB V der elektronischen Gesundheitskarte (eGK) in Verbindung mit einem elektronischen Heilberufsausweis. Hiervon abweichend können die Versicherten sich auch durch ein geeignetes technisches Verfahren authentifizieren.

Für Videosprechstunden im Rahmen der vertragsärztlichen Versorgung erfolgt die Authentifizierung des Versicherten durch das Vorzeigen der eGK gegenüber dem behandelnden Arzt. Dieses manuelle Verfahren soll weiterentwickelt werden. Aus § 291g Absatz 7 SGB V ergibt sich, dass die Kassenärztliche Bundesvereinigung und der Spitzenverband Bund der Krankenkassen im Benehmen mit der gematik bis Ende 2020 ein technisches Verfahren zur Authentifizierung der Versicherten im Rahmen der Videosprechstunde festzulegen haben. Dieses Verfahren kann auch derart ausgestaltet werden, dass ein Zugriff auf die bei den Krankenkassen gespeicherten Versichertendaten erfolgt, um so eine Authentifizierung im Rahmen der Videosprechstunde zu ermöglichen.

Auch im Kontext der Terminvermittlung unter 116117.de bzw. eTerminservice.de erfolgt eine Authentifizierung mittels eGK.[59] Alternativ dazu kann unter 116117.de eine E-Mail-Adresse eingegeben werden, die zu bestätigen ist und erst nach Bestätigung einen Vermittlungscode an den Nutzer, mit dem dieser einen Arzttermin über die

[59] Anlage 4a zum Bundesmantelvertrag Ärzte.

Plattform der Kassenärztlichen Vereinigungen vermittelt bekommt.

Die Anforderungen an Authentifizierungen im Rahmen des Kontaktes zwischen Krankenkassen und den Versicherten sind in der *GKV-SV Richtlinie Kontakt mit Versicherten*[60] festgelegt. Die Unterscheidung der Schutzanforderungsniveaus erfolgt auf Basis der Vertrauensniveaus der eIDAS-Verordnung analog der Technischen Richtlinie TR-03107-1 zwischen den Kategorien „normal", „substantiell" und „hoch", wobei die Kategorie „normal" im Sinne der TR-03107-1 dem Vertrauensniveau „niedrig" im Sinne der eIDAS-Verordnung zuzuordnen.[61] Für einen dauerhaften Zugang zu Portalen oder Anwendungen der gesetzlichen Krankenkassen ist gemäß Ziffer 6 eine Identifizierung des Berechtigten vor der Nutzung des Zugangs erforderlich, die dem jeweiligen Schutzanforderungsniveau der Daten entspricht, auf die der Versicherte zugreifen will. Die konkreten Anforderungen ergeben sich aus der TR-03147 des BSI. Die Anforderungen an Verfahren zur Authentifizierung von Versicherten gegenüber Portalen oder Anwendungen der Krankenkassen ergeben sich ebenfalls aus Ziffer 6 der GKV-SV Richtlinie.

Unterschiedliche Authentifizierungsverfahren dienen dabei der Sicherstellung der verschiedenen Schutzniveaus. Mit einem Ein-Faktor-Authentifizierungsverfahren, welches nicht transaktionsgebunden bzw. sitzungsgebunden ist, kann nur ein normales Schutzniveau erreicht werden, während substanziell oder hoch mittels einer Zwei-Faktor Authentifizierung abzubilden ist.

Perspektiven aus Europa

In anderen Ländern Europas sind digitale Anwendungen bereits seit einigen Jahren Teil des Versorgungsalltags von Patienten und Ärzten.

Dänemark-Login mit NemID

In Dänemark können Nutzerinnen und Nutzer über das dänische Gesundheitsportal sundhed.dk[62] auf ihre Gesundheitsdaten, unter anderen auf Diagnosen, Behandlungsverläufen, Medikamentenpläne, Röntgenergebnisse sowie Überweisungen an Spezialisten und Laborergebnisse zugreifen. Zur verlässlichen Identifizierung dient die persönliche Identifikationsnummer, die jeder Däne bei der Geburt erhält. Der Login auf die persönlichen Gesundheitsdaten kann auf sundhed.dk über NEMID[63] erfolgen, die ebenfalls mit der persönliche Identifikationsnummer verknüpft ist; für den Login-Vorgang müssen die User-ID von NEMID sowie das entsprechende Passwort eingegeben werden.[64] Eine Logdatei speichert die Zugriffe auf die Daten und ermöglicht so Transparenz und Nachvollziehbarkeit. Patienten können den Zugriff auf bestimmte Daten auch verweigern. Für viele Länder ist das dänische Modell ein „Best Practice"-Modell.

Österreich- Zugriff auf ELGA

In Österreich nutzen Patienten, Ärzte und Krankenhäuser die elektronische Gesundheitskarte, die ELGA, ein Informationssystem, welches den berechtigten Gesundheitsdiensteanbietern (ELGA-GDA) sowie den Patienten den orts- und zeitunabhängigen Zugang zu den entsprechenden ELGA-Gesundheitsdaten ermöglicht[65]. Die Überprüfung der Identität des ELGA Teilnehmers ist in § 18 des österreichischen Gesundheitstelematikgesetz 2012 – GTelG 2012 geregelt. Nach § 18 GTelG hat die Überprüfung der Identität der ELGA-Teilnehmer/innen in elektronischer Form unter Mitwirkung des ELGA-Teilnehmers/der ELGA-Teilnehmerin zu erfolgen. Dabei kann die Erhebung der Identitätsdaten u.a. durch die Prüfung der Gültigkeit der e-card in elektronischer Form und dem Auslesen von Daten der e-card mittels e-card-System oder unter Verwendung der Bürgerkarte nach § 2 Z 10 des österreichischen E-GovG erfolgen. Der Zugriff der ELGA Nutzer/Patienten auf die persönliche ELGA - der Authentifizierungsprozess - erfolgt über das österreichische Gesundheitsportal mittels Bürgerkarte bzw. Handy-Signatur. Nach dem Login sieht der Nutzer/Patient die in der ELGA gespeicherten Gesundheitsdaten und kann diese u.a. sperren, unwiderruflich löschen und speichern und darüber

[60] Richtlinie des GKV-Spitzenverbandes zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) vom 14.12.2018; abrufbar unter https://www.gkv-spitzenver-band.de/media/dokumente/krankenversicherung_1/telematik/sozialdaten/20190206_Richtlinie_217f_Abs4b_SGB_V.pdf.

[61] Ebd.

[62] https://www.sundhed.dk/.

[63] https://www.sundhed.dk/borger/min-side/.

[64] https://nemlog-in.dk/login.aspx/noeglekort.

[65] https://www.gesundheit.gv.at/elga/faq/wissenswertes, abgerufen am 18.02.2020.

hinaus Einsicht in die Protokolldaten nehmen und auf diese Weise sehen, welche ELGA-GDA aktuell Zugriff auf die persönlichen ELGA-Gesundheitsdaten haben.[66]

Estland- Identifizierungen mit nationaler eID

In Estland ist das Identifizierungs- und Authentifizierungsmittel im Gesundheitssektor die nationale eID (Karte oder mobile Lösung). Auch in Estland nutzen Patienten und Gesundheitsversorger ein nationales Gesundheitsportal, welches seit 2008 Teil der nationalen Dateninfrastruktur „X-Road" ist. Gesundheitsversorger sind an das System angebunden. Die Daten der Patienten sind darin zentral gespeichert. Auch hier haben Patienten Zugriff auf ihre Patientenakte, können geloggte Zugriffe von Dritten einsehen und ggf. Zugriffsberechtigungen einschränken. Auf die Patientenakte haben ebenso Gesundheitsversorger (eingeschränkten) Zugriff.

2. Anforderungen an digitale Identitäten im Gesundheitswesen - Ergebnisse der Debatte

Verlässliche digitale Identitäten im Gesundheitssektor

Digitale Identitäten sind ein zentraler Bestandteil für Gesundheitsanwendungen im digitalen Raum sein. Unter den Workshop-Teilnehmern bestand Einigkeit darüber, dass sie dem Schutz sensibler Gesundheitsdaten dienen, Vertrauen herstellen und Transparenz gewährleisten sollen. Verlässliche digitale Identitäten müssen die einschlägigen Bestimmungen des Datenschutzes und der Datensicherheit erfüllen.

Datenschutz und Datensicherheit

Gesundheitsdaten fallen nach der DSGVO in eine besondere Kategorie personenbezogener Daten, die aufgrund ihrer Sensibilität für den Einzelnen in besonderem Maße schützenswert sind.[67] Daher hat derjenige, der diese Daten verarbeitet, besondere technisch-organisatorische Maßnahmen zu ergreifen, um auch den Zugriff unberechtigter auf diese Daten auszuschließen. Um den hohen Datenschutzanforderungen zu entsprechen, sollten starke Authentifizierungsmechanismen implementiert werden. Die Sicherheit der Identifizierungs- und Authentifizierungslösungen im Gesundheitswesen ist eine Grundvoraussetzung für den Datenschutz. Vergleicht man die in der Praxis bestehenden Verfahren zur Identifizierung und Authentifizierung im Gesundheitswesen mit den Sicherheitsniveaus aus der eIDAS-Verordnung und TRs des BSI, so erreichen die meisten Lösungen für die Verarbeitung sensibler Gesundheitsdaten das Niveau „normal" oder „substanziell". Dies gilt für bestehende Verfahren wie das Bank-Ident für Ärzte (HBA), Auto-Ident bei Versichertenidentifizierung oder die SMS-Bestätigung als 2. Faktor. Das Niveau „hoch" lässt sich derzeit insbesondere durch den Einsatz der Online Ausweisfunktion des nPA, welche auf dem eIDAS-Sicherheitsniveau „hoch" notifiziert wurde, abbilden. Projekte wie OPTIMOS 2 (unter Konsortialführerschaft der Bundesdruckerei) wollen Identifizierungen und Authentifizierungen auf hohem Sicherheitsniveau mit Hilfe des Secure Elements des Smartphones ermöglichen. An das Smartphone werden bestimmte Attribute der Identität übertragen, die aus einer sicheren Quelle wie dem Personalausweis abgeleitet wurden, und in das Secure Element eingebunden.

Neben starken Authentifizierungsmechanismen ist ein eindeutiger Identifier von entscheidender Bedeutung. Im Bereich der Regelversorgung des Gesundheitswesens bilden die Telematik ID und die Krankenversicherungsnummer einen eindeutigen Identifier. Datenschutz und Datensicherheit bedingen sich im Hinblick auf verlässliche digitale Identitäten gegenseitig, denn unzureichend gesicherte IT-Systeme können keinen

[66] https://www.gesundheit.gv.at/elga/faq/wissenswertes, abgerufen am 25.02.2020.

[67] Erwägungsgrund 51 S. 1 DSGVO.

Datenschutz gewährleisten. In diesem Kontext adressierten die Teilnehmerinnen und Teilnehmer des Workshops die Herausforderung, dass neben Datenschutz und Datensicherheit auch eine intuitive Nutzbarkeit der Anwendungen gewährleistet werden muss. Denn digitale Anwendungen im Gesundheitswesen werden sich nur dann durchsetzen, wenn die angebotenen Lösungen auch im Alltag der Menschen praktikabel und einfach nutzbar sind. Wenn die Digitalisierung im Gesundheitswesen nicht aus der Nutzerperspektive gedacht wird, d.h. die ID-Lösungen für den Nutzer eine hohe Usability mit sich bringen, dann finden sie auch keine hohe Durchdringung. Dementsprechend müssen User Experience und Sicherheit in eine ausgewogene Balance gebracht werden. Der deutsche Gesundheitsmarkt ist mit rund 80 Millionen potenziellen Nutzern auch ein wichtiger Zielmarkt für nicht-europäische Digitalkonzerne, die mit Ihren Lösungen sektorübergreifende und intuitiv nutzbare digitale Identitäten anbieten.

Datensouveränität

Eine zentrale Frage, die der Workshop aufwarf, ist, wie die Datensouveränität von Patienten gewahrt und umgesetzt werden kann. Unter Datensouveränität verstehen wir im Allgemeinen die Fähigkeit des Nutzers, über die Verwendung seiner Daten selbst zu bestimmen sowie die Einhaltung eines angemessenen Datenschutz- und Datensicherheitsniveaus durch Anbieter und Betreiber von Diensten. Bei der Umsetzung von Datensouveränität in der digitalen Gesundheitsversorgung und Identifizierungslösungen ergibt sich die Frage, in welchem Maß und mit welchen Mitteln Patienten selbst über die Verwendung und die Sicherheit ihrer Daten bestimmen sollten. Einige Workshop-Teilnehmer befürworteten die Lösung, dass Nutzer / Patienten selbst über die Verwaltung ihrer Daten und damit auch selbst darüber entscheiden sollten, welche Daten sie freigeben, absichern bzw. offenlegen. In der Praxis setzt diese Möglichkeit jedoch ein gewisses Maß an Aufgeklärtheit auf Seiten der Patienten darüber voraus, wie ihre Daten verwendet und verarbeitet werden und wie sicher diese sind. Andere Workshopteilnehmer befürworteten daher, dass diese Entscheidungen nicht dem Patienten obliegen, sondern gesetzlich geregelt werden sollten. Die Frage, bis zu welchem Grad Patienten selbst entscheiden können, betrifft auch die Wahl des Identifizierungsdiensteanbieters. Es bestand Einigkeit darüber, dass Patienten und Gesundheitsversorger eine Auswahl zwischen unterschiedlichen Identifizierungslösungen haben sollten, die jeweils die notwendigen Datenschutz- und –Sicherheitsanforderungen einhalten.

Einheitlicher Rechtsrahmen- eIDAS-Verordnung im Gesundheitssektor

Mit der eIDAS-Verordnung wurden einheitliche Rahmenbedingungen für den grenzüberschreitenden Gebrauch elektronischer Identifizierungsmittel und Vertrauensdienste in den EU-Mitgliedstaaten sowie im Europäischen Wirtschaftsraum geschaffen. Sie ist ein Schlüsselelement zur Errichtung eines europäischen digitalen Marktes und dient der Stärkung des Vertrauens in digitale Dienste. Zur Erreichung dieser Ziele schafft die Verordnung eine gemeinsame Grundlage für sichere elektronische Interaktionen zwischen Bürgern, Behörden und Unternehmen. Der Anwendungsbereich der eIDAS-Verordnung ist in Art. 2 Abs. 1 eIDAS-Verordnung positiv normiert: zum einen findet die Verordnung Anwendung auf „*von einem Mitgliedstaat notifizierte elektronische Identifizierungssysteme*“ und zum anderen auf „*in der Union niedergelassene Vertrauensdienste*“. Zwingende gesetzliche Anwendung findet die eIDAS-Verordnung im Bereich des Gesundheitswesens, soweit die Leistungen von öffentlichen Stellen erbracht werden, zum Beispiel von öffentlichen Krankenhäusern oder der gesetzlichen Krankversicherung. Denn sie müssen nach Artikel 6 eIDAS-Verordnung eIDAS-konforme Identitäten anderer EU-Staaten anerkennen. Keine Geltung hat die eIDAS-Verordnung für private Leistungserbringer wie Ärzte und Apotheken oder auch für die privaten Krankenversicherungen.

Bei der eGK, die eine wesentliche Rolle im Kontext digitaler Identitäten im Gesundheitswesen innehat, handelt es sich nicht um ein notifiziertes Identifizierungssystem. Gleichwohl wird die Nutzung der Möglichkeiten des Identitätsnachweises nach der eIDAS-Verordnung im Sozialversicherungssystem auch über den öffentlichen

Bereich hinaus befürwortet[68]. Auch die gematik greift in ihren technischen Spezifikationen auf die eIDAS-Verordnung zurück, ebenso wie die Richtlinie des GKV Spitzenverbandes. Die eIDAS-Verordnung legt drei Sicherheitsniveaus zugrunde: *niedrig*, *substanziell* und *hoch*. Die eIDAS-Verordnung selbst ist als Rahmenwerk ausgestaltet und trifft dementsprechend auch keine Regelungen dazu, welches Sicherheitsniveau in welchem konkreten Anwendungsfall zugrunde zu legen ist. Die DSGVO, die basierend auf Art. 16 AEUV den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten dient, ordnet in Art. 9 DSGVO das grundsätzliche Verbot besonderer Kategorien personenbezogener Daten an. Dazu zählen nach der Art. 4 Nr. 15 DSGVO auch Gesundheitsdaten. Diese Daten gelten als sensible Daten, so dass ihnen eine besondere Schutzbedürftigkeit zugesprochen wird (vgl. EG 51 DSGVO). Im Zusammenhang mit ihrer Verarbeitung können erhebliche Risiken für die Grundrechte (Recht auf informationelle Selbstbestimmung und Recht auf körperliche Unversehrtheit) des Betroffenen ausgehen. Die Verarbeitung ist daher nur unter besonderen Voraussetzungen gestattet. Darüber hinaus finden im Kontext der Anwendungen der Telematikinfrastruktur die strengeren Regelungen des Sozialdatenschutzes der §§ 291 ff SGB V Anwendung. Dementsprechend wird für die Identifizierungen und Authentifizierungen für den Zugriff bspw. auf die ePA häufig das eIDAS-Vertrauensniveau *hoch* gefordert, auch wenn dies nicht ausdrücklich gesetzlich geregelt ist. Danach wäre ein Zugriff auf Gesundheitsdaten der ePA insbesondere mittels der Onlineausweisfunktion des nPA möglich.

Einigkeit bestand unter den Teilnehmern, dass Authentifizierungen im Gesundheitswesen für die Nutzer im Alltag durch nicht zu hohe Barrieren erschwert werden dürfen. Wenn die Nutzungshürden zu hoch sind, finden die digitalen Anwendungen im Gesundheitswesen keine Verbreiterung. Entsprechend existieren derzeit auch Lösungen der Krankenkassen in Form von elektronischen Patientenakten, die das eIDAS-Sicherheitsniveau substanziell abbilden, um Usability und Sicherheitsanforderungen zu verbinden.

Sektorübergreifende digitale Identität

Es bestand Einigkeit unter den Teilnehmern darüber, dass das derzeitige System verschiedener nicht interoperabler digitaler Identitäten überwunden werden müsse. Eine Ablösung aller verwendeten Identitäten durch eine einheitliche digitale Identität für alle Anwendungen im Gesundheitssektors erscheint kurz- und mittelfristig nicht machbar. Jedoch könnte das System durch eine virtuelle Identität für das Gesundheitswesen als föderierte Identität ergänzt werden, die vorhandene Identitäten verknüpft. Sie sollte mit sektorübergreifenden Lösungen kompatibel, anschlussfähig zu eIDAS und mit Credentials im Smartphone verknüpft sein.

3. Empfehlungen

Empfehlung 1

Patienten und Nutzern sollte ein einfaches Identitäten-Management für alle Anwendungen des Gesundheitswesens zur Verfügung gestellt werden. Es könnte als föderierte digitale Identität ausgestaltet werden, die auf Wunsch der Nutzer die verschiedenen Identitätssysteme über offene Schnittstellen verknüpft.

Empfehlung 2

Übergreifendes Identitätsmanagement im Gesundheitswesen sollte sich an sektorübergreifenden Standards und der eIDAS-Verordnung orientieren.

[68] Der Digitalausschuss im Bundesversicherungsamt (neu: Bundesamt für Soziale Sicherung, BAS), 8.2, S.43. https://www.bundesamtsozialesicherung.de/fileadmin/redaktion/Digitalausschuss/2019-10-31_Bestandsaufnahme_BVA_Digitalisierung_V1.3.pdf (abgerufen am 17.03.2020).

Fazit

Die unterschiedlichen Debatten haben gezeigt, dass digitale Identitäten sektorübergreifend Voraussetzung für digitale Geschäftsmodelle wie für die digitale Daseinsvorsorge sind. Aus den Ergebnissen lassen sich als Fazit folgende übergreifende Empfehlungen ableiten.

Nutzbarkeit: Digitale Plattformen und insbesondere Identitätslösungen müssen sich vor allem an den Bedürfnissen der Endanwender orientieren. Die leichte und intuitive Nutzbarkeit muss im Vordergrund stehen, um eine breite und Anwendungs-übergreifende Nutzung zu ermöglichen.

Sicherheit: Digitale Identitäten müssen verlässlich sein und angemessene Datenschutz- und Datensicherheitsstandards aufweisen. Sie müssen je nach Schutzprofil unterschiedliche Sicherheitsniveaus gewährleisten, wie sie der risikobasierte Ansatz der europäischen eIDAS-Verordnung vorsieht. Die Sicherheit digitaler Identitäten sollte mit der Nutzbarkeit vereinbar sein. Zu hohe Sicherheitsanforderungen dürfen die Verbreitung nicht behindern.

Interoperabilität und Offenheit: Digitale Identitäten müssen mittel- und langfristig sektorübergreifend nutzbar sein und auf einheitlichen, offenen und interoperablen Standards basieren. Digitale Plattformen für das Identitäten-Management sollten einen diskriminierungsfreien Zugang zu Diensten und universelle Anwendbarkeit ermöglichen. Die technische Offenheit einer Plattform erleichtert ebenfalls die Verknüpfung von Angeboten und senkt die Markteintrittshürde für Diensteanbieter. Sie ist somit auch aus marktwirtschaftlicher Perspektive vorteilhaft.

Digitale Souveränität: Digitale Identitäten als Schlüssel digitaler Geschäftsmodelle sind von besonders hoher Bedeutung für die Steuerbarkeit der digitalen Transformation in Geschäftsmodellen, Daseinsvorsorge und staatlichen Leistungen. Eine Beherrschung des Marktes digitaler Identitäten durch globale Plattformanbieter würde mit einem Verlust an Steuerungsfähigkeit für deutsche und europäische Politik und Wirtschaft einhergehen. Eine Strategie der digitalen Souveränität ist bei digitalen Identitäten von zentraler Bedeutung.

Gesamthafte Identitäten-Strategie von Staat und Wirtschaft: Zukünftig wird entscheidend und erforderlich sein, eine gesamthafte Identitäten-Strategie zwischen Staat und Wirtschaft zu erarbeiten und Rahmenbedingungen festzulegen, an denen sich Plattformen einerseits und die sie nutzenden Institutionen aus Staat und Wirtschaft andererseits orientieren können. Deutschland sollte dem Beispiel anderer europäischer Staaten folgen und eine gesamtheitliche Strategie und Kooperation von Staat und Wirtschaft festlegen.