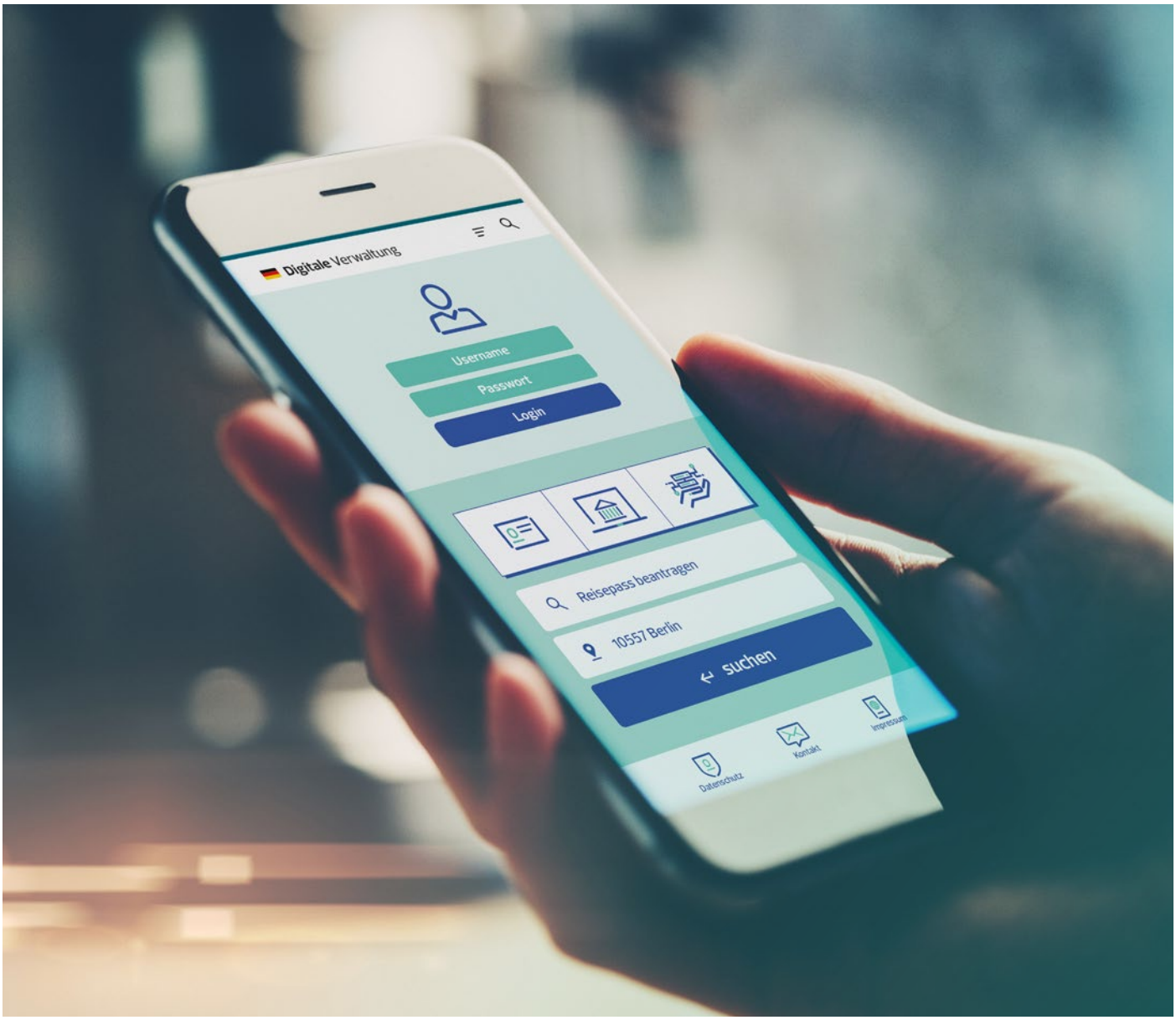
iRights.Lab
Think Tank für die digitale Welt

BUNDESDRUCKEREI

STUDIE

Zukunft E-Government.

Vorschläge für eine bürgerfreundliche und sichere Digitalisierung der Verwaltung



STUDIE

Zukunft E-Government.

Vorschläge für eine bürgerfreundliche und sichere Digitalisierung der Verwaltung

INHALT

EXECUTIVE SUMMARY

Deutschland hat Nachholbedarf im E-Government. Während sich die meisten Deutschen wünschen, Verwaltungsvorgänge künftig auch online erledigen zu können, bleiben die derzeitigen digitalen Verwaltungsstrukturen hinter den eigenen Ansprüchen zurück. Vor diesem Hintergrund entwickelt die vorliegende Studie die grundlegenden Parameter für eine umfassende und sichere E-Government-Architektur als Grundversorgungsprojekt für die Bundesrepublik Deutschland. Beleuchtet werden die entscheidenden technischen, rechtlichen, politischen sowie gesellschaftlichen Aspekte. Ausschlaggebend für das Gelingen eines solchen Vorhabens ist die Schaffung und Implementierung sicherer digitaler Identitäten.

Der Erfolg der digitalen Transformation in Deutschland wird vor allem davon abhängen, ob an die existierenden Strukturen angeknüpft werden kann. Ein schrittweises Vorgehen ist dabei disruptiven Prozessen vorzuziehen. Nur so können die Interessen aller Betroffenen von Beginn an in die Planungen einbezogen werden. Das gilt insbesondere für die Stakeholder innerhalb der Verwaltung selbst.

Die staatlichen Stellen sollten sich ausreichend eigenes technisches Wissen aneignen und durch entsprechende Einstellungspraxis erwerben, um große Teile der E-Government-Infrastruktur in Eigenregie umsetzen und implementieren zu können. Es sollten nicht mehr Teilbereiche als notwendig an private Akteure ausgelagert werden. Der Staat muss stets Herr des Verfahrens bleiben. Gegenüber den Bürgern kann er dabei auf seiner besonderen Vertrauensposition aufbauen. Zudem kann er nur so die Beschäftigten in der Verwaltung vom Start der Umsetzung an mitnehmen.

Noch entscheidender ist jedoch der Ansatz der Bürgerzentriertheit. Die Bürger müssen die digital angebotenen Verwaltungsdienstleistungen intuitiv nutzen können. Weiterhin müssen sie den Leistungen vertrauen können. Für die Arbeit einer digitalen Verwaltungsinfrastruktur werden personenbezogene Bürgerdaten benötigt; doch die Bürger müssen stets die Datensouveränität behalten. Mit dem hier skizzierten Bürgerportal können sie selbst Zugriffe auf die eigenen Daten erteilen und das Recht dazu wieder entziehen.

Die entworfene E-Government-Infrastruktur folgt den Grundprinzipien:

- Nutzerfreundlichkeit
- Datensouveränität
- Sicherheit

Diese werden umgesetzt durch folgende Bausteine:

- Authentifizierung und Autorisierung von Benutzern
- Zentrale Zugriffsplattform mit integrierten Vertrauensdiensten
- Single Sign-on für den Zugriff auf unterschiedliche Systeme und Ressourcen mit einer einzigen Identität
- Zentralisierte Verwaltung von Identitäten und Zugriffsberechtigungen
- Nutzerzentrierung, d. h. souveräne Verteilung und Kontrolle von Zugriffsrechten auf Dokumente durch Bürger und Unternehmen

Dabei ist eine den höchsten Standards genügende Datensicherheitsarchitektur unabdingbar. Ihr Kernstück ist eine sichere digitale Identität, mit der Bürger gegenüber der Verwaltung online auftreten können. Sie muss stabil und darf nicht korrumpierbar sein. Zudem sind eine nachgelagerte Authentifizierung und das Prinzip des Single Sign-on entscheidend. Dank diesem können Bürger sämtliche verfügbaren Dienste mit einem einzigen Account am heimischen Computer oder per mobilem Endgerät nutzen.

Ein weiterer Baustein der Infrastruktur ist die E-Government-Plattform mit integrierten Vertrauensdiensten. Die Serviceplattform dient als zentrale Kommunikationsschnittstelle zwischen den Bürgern/Unternehmen und der Verwaltung.

Sie setzt sich aus folgenden Komponenten zusammen:

- Sicherer Speicher für private Daten und Dokumente
- Möglichkeit zur Abfrage und automatischen Übermittlung von Dokumenten und anderen Daten in passende Prozesse
- Authentizitätsprüfung der Daten und Dokumente

Die Funktionsweise des Datenspeichers setzt die Datensouveränität des Bürgers um. Dies entspricht den Erwartungen der Nutzer

und den Anforderungen der Datenschutz-Grundverordnung im Sinne des „Privacy by Design"-Ansatzes: vollständige Transparenz für den Nutzer und keine Einsichtsmöglichkeit für andere (engl. „Zero Knowledge"), jedenfalls solange diese keine entsprechende Berechtigung durch den Nutzer erhalten haben oder diese aufgrund einer sonstigen rechtlichen Grundlage besitzen. In besonderem Maße gilt dies für die sensible Datenablage.

Zusätzlich zu den technischen Aspekten der E-Government-Architektur müssen bestehende rechtliche Rahmenbedingungen wie die europäische eIDAS-Verordnung eingehalten und notwendige Novellierungen auf den Weg gebracht werden. Das gilt insbesondere für den Datenaustausch zwischen Behörden. Darüber hinaus muss die Bevölkerung früh auf E-Government vorbereitet werden – und die Verwaltung ist umfassend und fortlaufend zu qualifizieren.

1 EINLEITUNG

Wer in Großstädten oder Ballungsgebieten einen neuen Reisepass beantragen will, muss oft wochenlang auf einen freien Termin bei der zuständigen Behörde warten.[1] Wer auf dem Land wohnt und einen solchen Antrag stellen möchte, hat es oft leichter, einen Termin zu finden – der Weg zur nächstgelegenen Behörde ist jedoch mitunter weit, insbesondere seitdem viele Ämter im Zuge von Verwaltungsreformen zusammengelegt worden sind. Behördengänge sind zeitintensiv und anstrengend – und wer kann, schiebt sie häufig auf, bis sie unumgänglich werden. Zudem müssen sich natürlich alle Bürger* nach den Öffnungs- und Sprechzeiten der Behörden richten. Nur wenigen Arbeitnehmern ist dies problemlos möglich.

1 Siehe für das Land Berlin „Berliner Verwaltung soll besser werden: Umsetzung dauert", Berliner Morgenpost, 7. März 2018, *https://www.morgenpost.de/berlin/article213651921/Berliner-Verwaltung-steht-vorgewaltigen-Veraenderungen.html.*

* Die männliche Schreibweise wird ausschließlich aus Gründen der Leserfreundlichkeit verwendet. Wir weisen an dieser Stelle ausdrücklich darauf hin, dass wir hiermit immer beide Geschlechter meinen.

Angesichts all dessen stellt sich fast unweigerlich die Frage: Lassen sich Behördengänge nicht besser und unkomplizierter erledigen mitten im digitalen Zeitalter?

Aufbauend auf dieser Ausgangsfrage werden in der vorliegenden Studie die grundlegenden Parameter für eine in Deutschland zu errichtende E-Government-Infrastruktur entwickelt und dargelegt. Darüber hinaus befasst sich das Arbeitspapier mit den technischen Grundkomponenten sowie den rechtlichen, politischen, gesellschaftlichen und ethischen Aspekten, die zu klären sind.

1.1 Der Wunsch nach bequemer und vertrauenswürdiger digitaler Verwaltung

„Deutsche warten auf den digitalen Staat" überschrieb das Handelsblatt eine Meldung vom Dezember 2017, in der es auf eine Studie von PricewaterhouseCoopers verwies.[2] Laut dieser repräsentativen Umfrage wären neun von zehn Bürgern bereit, Verwaltungsvorgänge in Zukunft auf digitalem Wege zu erledigen.[3] Ebenso viele wünschen sich, dies mittels eines zentralen Bürgerkontos abwickeln zu können[4] – also anhand eines individuellen digitalen Nutzerprofils, in dem alle Verwaltungsvorgänge zentral, transparent und kostenlos zusammenlaufen.[5]

Die Befragung verdeutlicht, mit welchen Faktoren E-Government-Lösungen beim Bürger punkten können: Die Bürger müssen glaubwürdig vermittelt bekommen, dass sie dem Staat in Bezug auf den Schutz der eigenen personenbezogenen Daten vertrauen können. Von diesem Vertrauen ist somit das ganze Projekt der digitalen Transformation der Verwaltung abhängig. Dabei werden in diesem Punkt gewichtige Bedenken angemeldet. Viele Bürger fürchten sich explizit vor Datenmissbrauch oder -manipulation oder haben Angst vor Zugriffen auf die online gespeicherten sensiblen Datenbestände durch unbefugte

2 Dana Heide, „Deutsche warten auf den digitalen Staat", Handelsblatt, 12. Dezember 2017, *https://www.handelsblatt.com/politik/deutschland/e-government-deutsche-warten-auf-den-digitalen-staat/20697800.html.*

3 PwC, Die vernetzte Verwaltung. Digitalisierung aus der Bürgerperspektive, September 2017, *https://www.pwc.de/de/offentliche-unternehmen/die-vernetzte-verwaltung-2017.pdf*, S. 8.

4 Ebd., S. 9.

5 Ebd., S. 17.

Dritte.[6] Sogar viele, die ein Bürgerkonto ausdrücklich befürworten, sorgen sich: Sechs von zehn Personen dieser Gruppe haben Bedenken bei der Verwendung ihrer personenbezogenen Daten, 43 Prozent haben grundsätzliche datenschutzrechtliche Bedenken.[7]

6 Ebd., S. 26.

7 Ebd., S. 24.

1.2 Nachholbedarf in Deutschland

Die Sorgen der Bürger sind jedoch nicht der Hauptgrund dafür, dass Deutschland beim E-Government zurückliegt, besonders im Vergleich zu anderen europäischen Ländern. In einer Untersuchung von 2016, in der die Europäische Kommission den Stand des E-Governments in den Mitgliedsstaaten der Europäischen Union bewertete, ordnete sie Deutschland auf Platz 20 von 28 ein.[8] Zudem gehörte Deutschland laut EU-Kommission zu jenen Ländern, die in den vergangenen Jahren praktisch keine Fortschritte bei E-Government-Infrastrukturen verzeichnen konnten.[9]

Was sind die Gründe dafür? Gemäß E-Government-Monitor der Initiative D21 nutzen in Deutschland lediglich 40 Prozent der Bevölkerung digitale Verwaltungsdienste. In Österreich sind es 74 Prozent, in der Schweiz immerhin 61 Prozent.[10] Diese großen Unterschiede sind bei genauerem Hinsehen eine Konsequenz der Qualität und Verfügbarkeit des jeweiligen Angebots. So kommt die Bertelsmann Stiftung zu dem Schluss, dass digitale Dienstleistungsangebote in Deutschland schlicht nicht die Erwartungen der Bürger treffen.[11]

In der Tat bleiben die digitalen Dienstleistungen der Behörden sehr oft hinter dem technisch Machbaren zurück. Bislang dienen die Online-Angebote der Verwaltung in Deutschland eher der Vorbereitung von Verwaltungsvorgängen, nicht aber deren Abwicklung.[12] So können Bürger sich auf den Webseiten der jeweils zuständigen Behörden meist gut über die Voraussetzungen von Anträgen, Meldungen oder anderen Vorgängen informieren und auch die entsprechenden Formulare herunterladen – der Weg zur Behörde selbst bleibt ihnen im Normalfall dennoch nicht erspart.

Während in Deutschland die Hälfte aller Verwaltungsdienstleistungen nicht online abgewickelt werden kann, sind es in den E-Government-Vorzeigeländern Estland und Österreich höchstens 15 Prozent.[13]

8 Siehe Heide, Handelsblatt 2017; EU-Kommission, eGovernment Benchmark 2016. A turning point for eGovernment development in Europe? Background Report (Vol. 2), 2016, *https://bit.ly/2v5F6F5*.

9 EU-Kommission 2016, S. 100.

10 Initiative D21, E-Government-MONITOR, E-Government-Nutzer in der Bevölkerung, *http://www.egovernment-monitor.de/e-government/nutzung.html*.

11 Bertelsmann Stiftung (Hg.), Digitale Transformation in der Verwaltung. Empfehlungen für eine gesamtstaatliche Strategie, 2017, *https://bit.ly/2DvzY0T*, S. 7.

12 PwC 2017, S. 23.

13 Bertelsmann Stiftung 2017, S. 15.

1.3 Die Vorhaben der Bundesregierung

Wo also besteht Handlungsbedarf? Laut Bertelsmann Stiftung fehlt es beim E-Government bislang an kohärenter gesamtstaatlicher strategischer Steuerung.[14] Dabei hat die Bundesregierung den dringenden Bedarf erkannt und sieht auch ihre Zuständigkeit: Schon 2013 wurde auf ihre Initiative das E-Government-Gesetz erlassen, das die Möglichkeit elektronischer Kommunikation mit der Verwaltung fördern soll. Es verpflichtet die Verwaltung unter anderem, einen elektronischen Zugang zu diesem Zweck zu eröffnen. Zudem soll schrittweise mittels sicherer Technologien wie der qualifizierten elektronischen Signatur oder der Online-Ausweisfunktion die Schriftform ersetzt werden, die in vielen Verwaltungsvorschriften noch immer verbindlich ist.[15]

14 Ebd., S. 7.

15 Bundesministerium des Innern, für Bau und Heimat, E-Goverment-Gesetz, *https://bit.ly/2v4rl9T*.

Eingebettet ist das Gesetz in das Regierungsprogramm „Digitale Verwaltung 2020". Dies soll Behörden dabei unterstützen, mit konkreten Projekten die Digitalisierung umzusetzen. Diese zumeist langfristig angelegten Projekte betreffen in erster Linie zentrale technische Infrastrukturen, die es Bürgern ermöglichen, leichter mit der Verwaltung in Kontakt zu treten. Eines der prominenteren Einzelvorhaben ist der sogenannte Portalverbund. Mit diesem sollen Bund und Länder ihre Verwaltungsportale verknüpfen, um Bürgern einen zentralen, leicht und sicher verfügbaren Zugang zu Verwaltungsdiensten im Netz anzubieten.[16]

Insbesondere die Bundesregierung hat im Koalitionsvertrag zwischen CDU, CSU und SPD vom Februar 2018 an mehreren Stellen deutlich gemacht, dass sie die digitale Transformation der Verwaltung in Deutschland in dieser Legislaturperiode beschleunigen will.[17]

So sprechen sich die Koalitionsparteien ausdrücklich dafür aus, ein „digitales Bürgerportal", also ein Bürgerkonto, zu entwickeln und einzurichten, das „praktisch alle" Verwaltungsdienstleistungen künftig elektronisch verfügbar macht. Es solle von nun an das Prinzip „Digital First" gelten.[18] Im Abschnitt „Auf dem Weg in die digitale Verwaltung" des Koalitionsvertrags wird dieses Vorhaben näher ausgeführt. So soll es Lösungen für die einfache und sichere elektronische Identifizierung der einzelnen Bürger im Netz geben, ohne die E-Government insbesondere im Sinne der Abwicklung von Verwaltungsakten nicht möglich wäre. Zudem soll der geplante Portalverbund geeignete zentrale und dezentrale Verwaltungsportale verknüpfen. Dieser Portalverbund soll mit den Bürgerkonten so verbunden werden, dass die Bürger stets sehen können, „welche Daten beim Staat vorliegen [und] welche Behörde darauf Zugriff genommen hat", so dass sie vermehrte Kontrolle über den Umgang mit den eigenen personenbezogenen Daten zu jedem Zeitpunkt behalten.[19]

16 Bundesregierung, Digitalisierung der Verwaltung voranbringen, *https://bit.ly/2qyT4g4*; Bundesministerium des Innern, für Bau und Heimat, Portalverbund digitaler Verwaltungsdienstleistungen: einfach, schnell und sicher, *https://bit.ly/2BkJ3a1*.

17 Ein neuer Aufbruch für Europa. Eine neue Dynamik für Deutschland. Ein neuer Zusammenhalt für unser Land. Koalitionsvertrag zwischen CDU, CSU und SPD, Berlin, 7. Februar 2018, *https://bit.ly/2LF4Cvd*.

18 Ebd., S. 12.

19 Ebd., S. 45.

Die Idee des Bürgerportals

Eine Möglichkeit sicherer digitaler Identifikation ist laut Koalitionsvertrag der elektronische Personalausweis, der zu einem „universellen, sicheren und mobil einsetzbaren Authentifizierungsmedium" werden soll. Dazu soll an der Benutzerfreundlichkeit gearbeitet und eine Opt-in-Lösung implementiert werden, welche die Nutzung für E-Government-Funktionen von der Zustimmung der Bürger abhängig macht. Auf diese Weise wäre das „Once only"-Prinzip möglich: also die Verknüpfung der personenbezogenen Daten über verschiedene behördliche Register, so dass unterschiedliche Behörden, aber potenziell auch privatwirtschaftliche Dienstleister darauf zugreifen können.[20]

20 Ebd., S. 46.

1.4 Interessen und Erwartungen an die E-Government-Infrastruktur

Von einer sicheren und umfassenden E-Government-Infrastruktur würden viele Personengruppen profitieren. Die wichtigsten Stakeholder und ihre jeweiligen Interessen werden daher im Folgenden kurz benannt.

1.4.1 Bürger

Zunächst sind die Bürger zu nennen. Ihr Verhältnis zum Staat und zu seiner Verwaltung wird sich wahrscheinlich grundlegend ändern, sobald die Interaktion mit Behörden hauptsächlich digital vollzogen wird. Die Bürger möchten durch die Digitalisierung der Verwaltung vor allem ihren Aufwand beim Erledigen von Behördenangelegenheiten verringern. Dabei geht es zum einen um den Faktor Zeit. Hier werden wahrscheinlich die größten Erwartungen liegen, wenn die Bürger künftig nicht mehr auf einen freien Termin warten müssen, sondern sich den Weg zum Amt ersparen können und zeitlich flexibel sind. Wird das Bürgerkonto zudem kostenfrei angeboten, können Behördenangelegenheiten günstiger abgewickelt werden. Die Bürger müssten beispielsweise weder für Benzin noch Bahn- oder Busticket zahlen, um zur Behörde zu kommen. Dabei wären angesichts der gängigen Geschäftsmodelle im Internet (etwa soziale Medien oder journalistische Angebote) wahrscheinlich nur wenige Bürger bereit, für die Nutzung des Angebots selbst (von kostenpflichtigen Verwaltungsdienstleistungen im Einzelfall abgesehen) einen regelmäßigen Geldbetrag zu leisten.

Darüber hinaus erwarten die Bürger, dass das Bürgerkonto intuitiv zu bedienen und mobil verfügbar ist. Außerdem sollte man vom Konto aus zentral auf sämtliche Angebote zugreifen können. Sind diese Kriterien erfüllt, so könnte diese Gruppe interessiert sein, das Bürgerkonto mit seiner damit verknüpften digitalen Identität als „digitalen Generalschlüssel" für die Interaktion mit privatwirtschaftlichen Angeboten im Internet zu nutzen. Ein solches Single Sign-on als vertrauensvoller Zugang zur digitalen Welt könnte bereits bestehende Angebote von großen Plattformanbietern wie Google oder Facebook ersetzen, mittels derer sich heute viele Internetnutzer auf verschiedensten Webseiten anmelden. Diese mit kommerziellen Plattformen verknüpften digitalen Identitäten sind zwar bequem zu nutzen. Doch viele Bürger fühlen sich zunehmend unwohl dabei, den privaten und global operierenden Unternehmen weitere personenbezogene Daten zur Verfügung zu stellen.[21] Ein quasi öffentliches Single Sign-on als Alternative zum Login

21 Tino Tezel, „Verbraucher misstrauen Unternehmen beim Datenschutz", Datenschutzbeauftragter INFO, 14. Januar 2016, *https://bit.ly/2KNLpDb.*

via Facebook oder Google, das als Teil des Bürgerkontos geschaffen wird, könnte eine Option sein, den Erwartungen der Bürger gerecht zu werden und die Attraktivität des Bürgerkontos deutlich zu erhöhen.

Für diese Szenarien braucht es natürlich hohe Datenschutz- und -sicherheitsstandards. Zudem müssen die Bürger Vertrauen haben und die Technik selbst muss stets absolut reibungslos funktionieren. Hier kann sich ein staatliches Angebot klar von privatwirtschaftlichen Anbietern abgrenzen bzw. eine mindestens gleichwertige Alternative darstellen. Gerade aufgrund der Datenschutzvorfälle vergangener Jahre werden die Nutzer eine größere Kontrolle über die eigenen, auf E-Government-Plattformen hinterlegten Daten fordern. Damit eng verknüpft müssen sie stets nachvollziehen können, wer wann und zu welchem Zweck auf die Daten zugreift.

1.4.2 Wirtschaft

Auch die Privatwirtschaft in Deutschland hat ein Interesse an einer funktionierenden und umfassenden E-Government-Infrastruktur. Zunächst können sie damit ihre eigenen Interaktionen mit der Verwaltung effizienter gestalten, etwa um neue Unternehmen anzumelden, Gewerbe an- oder umzumelden, Umzüge des Unternehmenssitzes abzuwickeln, Maßnahmen zur Arbeitssicherheit umzusetzen, Visa-Angelegenheiten beim Arbeitskräfteeinsatz im Ausland zu regeln oder sonstige Anträge auf Verwaltungsakte zu stellen. Darüber hinaus könnten gerade deutsche Unternehmen daran interessiert sein, die der E-Government-Struktur zugrunde liegende sichere digitale Identität in eigene Angebote einzubinden, um von dem hohen Vertrauen in die bereitgestellte Architektur zu profitieren. Diese Möglichkeit könnte insbesondere für Banken oder Versicherungsunternehmen nutzbringend sein.

1.4.3 Öffentliche Institutionen und Behörden

Richtig entwickelt und implementiert, bietet die digitale Transformation die Chance, auch öffentliche Aufgaben effizienter, transparenter und effektiver zu erbringen,[22] wovon auch Staat und Verwaltung selbst profitieren.

22 Bertelsmann Stiftung 2017, S. 15.

So ist den Verwaltungsinstitutionen auf allen Ebenen (Bund, Länder, Kommunen) daran gelegen, administrative Abläufe insbesondere bei der Interaktion mit Bürgern sowie Unternehmen zu vereinfachen und effizienter zu gestalten. Auf diesem Wege können erhebliche Kosten gespart werden. Auf Bundesebene kommt die Erwartung hinzu, durch möglichst bundeseinheitliche Lösungen bei der Umsetzung des Vorhabens die allgemeine Rechtssicherheit bei E-Government-Angeboten zu erhöhen. Als Hauptakteure der konkreten Umsetzung vor Ort versprechen sich dagegen vor allem die öffentlichen Institutionen auf Länder- und kommunaler Ebene signifikante Effizienzsteigerungen, durch die mittel- bis langfristig die eigenen Haushalte entlastet werden können.

Die Behörden selbst als eigentliche Anbieter der Dienstleistungen des E-Governments erwarten vor allem, dass sich die bereitgestellte Infrastruktur mit möglichst geringen

Reibungsverlusten in die bestehenden Prozesse eingliedert und somit tatsächlich Verwaltungsabläufe vereinfacht und effizienter gestaltet werden. Darüber hinaus besteht ein Interesse an umfassender und nachhaltiger Implementierung, die Raum für Nachsteuerung und Weiterentwicklung lässt.

1.5 Skepsis und Ambivalenz gegenüber technologischer Innovation

Es besteht – vielleicht paradoxerweise – trotz des Wunschs nach einer funktionierenden elektronischen Verwaltung gleichwohl eine Skepsis gegenüber technologischen Innovationen. In einer aktuellen Studie zur Nutzung digitaler Assistenten wurden in ganz Europa Bürger befragt, was für sie bei der Akzeptanz solcher Assistenten am wichtigsten sei. An oberster Stelle stehen auch hier der Datenschutz bzw. die Frage des Umgangs mit personenbezogenen Daten.[23] Es folgt die Sicherheit des Systems vor Zugriffen durch Unbefugte und kriminelle Hacker.[24]

Eine weitere Untersuchung zur Innovationsforschung und zur Früherkennung von Fehlentwicklungen in der Technologie, durchgeführt von der Deutschen Akademie der Technikwissenschaften,[25] bestätigt die zentrale Bedeutung der Aspekte Sicherheit[26] und Datenschutz[27] beim Umgang der Bevölkerung mit Technologie. Skepsis besteht auch bei der Nützlichkeit von Digitalisierung. Nur für ein Viertel der Befragten (24,6 Prozent)[28] löst Technik mehr Probleme, als sie schafft. Das zeigt: Bei der Digitalisierung der Verwaltung werden damit einhergehende Veränderungen von den Bürgern nur dann angenommen, wenn sie davon überzeugt werden können, dass die Technologie tatsächlich der Lösung von Problemen dient und sie eine klare, greifbare Verbesserung spüren.

Insgesamt zeigen die empirischen Erhebungen eine generelle Ambivalenz in der Nutzung digitaler Technologien. Dem Willen zur Nutzung steht stets die Erwartungshaltung bei Datenschutz und Sicherheit gegenüber. So gehen Bürger beispielsweise mehrheitlich davon aus, an Komfort zu gewinnen (54,5 Prozent),[29] befürchten jedoch zugleich, die Hoheit über ihre eigenen personenbezogenen Daten zu verlieren (60,6 Prozent).[30] Sorgen um die Datensicherheit machen sich vor allem jüngere Befragte, Höhergebildete, Personen mit einer technisch-naturwissenschaftlichen Ausbildung sowie diejenigen Befragten, die sich sozial oberhalb der Mittelschicht einordnen. Zudem wird die Abhängigkeit von bestimmten Systemen und deren Herstellern als negativ empfunden und als Grund dafür angegeben, von der Nutzung Abstand zu nehmen.[31]

Die Skepsis und ambivalente Grundhaltung können den Erfolg der digitalen Transformation in der Verwaltung hemmen.

Diese skeptische Grundhaltung hat sich in den vergangenen Monaten eher verstärkt. Ausgelöst wurde dies durch einige schwerwiegende Datenskandale, über die teilweise monatelang berichtet wurde. Das bekannteste Beispiel ist die Rolle der größten Social-Media-Plattform Facebook bei der Information über Wahlprozesse und -kampagnen in

23 Osborne Clarke (Hg.), The European connected consumer: A life lived online, April 2018, *http://www.osborneclarke.com/wp-content/uploads/2018/04/OC-Connected-Consumer_04-2018.pdf*, S. 17. Auf Platz 1 mit 34 Prozent in Europa (sogar etwas höher in Deutschland mit 35 Prozent der Nutzer).

24 Ebd., S. 17. Auf Platz 2 mit 33 Prozent in Europa und auch speziell in Deutschland.

25 acatech, München, und Körber-Stiftung, Hamburg (Hg.), Technik-Radar 2018. Was die Deutschen über Technik denken, *https://www.koerber-stiftung.de/fileadmin/user_upload/koerber-stiftung/redaktion/technikradar/pdf/2018/Technikradar-2018_Langfassung.pdf*

26 Ebd., S. 32. 67 Prozent der Befragten befürchten sogar, dass Internetkriminelle in den Verkehr von selbstfahrenden Autos eingreifen und Störungen oder Unfälle verursachen werden.

27 Ebd., S. 33. 65 Prozent der Befragten finden es störend, wenn beim vollautomatischen Fahren persönliche Daten gesammelt werden.

28 Ebd., S. 17.

29 Ebd., S. 8.

30 Ebd., S. 30.

31 Ebd., S. 41. Beispielsweise sind 66,3 Prozent der Befragten der Meinung, dass die Nutzung von Smarthome-Technologie zu einer Abhängigkeit von System oder Herstellern führt.

den USA und in europäischen Ländern. So ist die Ablehnung der Bürger gegenüber der Weitergabe ihrer Daten durch Facebook an dritte Parteien seit der Berichterstattung über den Fall Cambridge Analytica stark angestiegen.[32] Dabei beruht das gesamte Geschäftsmodell von Facebook unter anderem darauf, die durch die Nutzer bereitgestellten bzw. generierten Daten weiterzuveräußern. Das Unternehmen selbst hat seine eigene Praxis nicht kürzlich geändert. Neu ist lediglich, dass den Nutzern diese Tätigkeit und damit verbunden ihre fehlende Kontrolle über die eigenen Daten bewusst geworden sind.

32 Vgl. umfassend Wikipedia, Facebook–Cambridge Analytica data scandal, *https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal.*

Mit anderen Worten: Je mehr die Nutzer über den Missbrauch der Daten erfahren, desto größer ist ihre Ablehnung. Die zuvor eher sorglose Haltung vieler Nutzer in Bezug auf Sicherheit und Datenverarbeitung war eine Folge schlichter Unkenntnis über Sicherheitslücken der genutzten Plattformen und den tatsächlichen Gebrauch der personenbezogenen Daten.

Hinzu kommt ein gesteigertes Bewusstsein für Datenschutz, das auch mit legislativen Entwicklungen zusammenhängt. So hat das Inkrafttreten der neuen europäischen Datenschutz-Grundverordnung zu einer vermehrten Auseinandersetzung der Verbraucher mit den verschiedenen Aspekten des Datenschutzes und der Datensicherheit geführt.

1.6 Die Prämissen der Untersuchung

Die vorliegende Studie untersucht die Parameter und Voraussetzungen, die zu erfüllen sind, um eine umfassende E-Government-Plattform für Deutschland als Grundversorgungsprojekt zu entwickeln und umzusetzen. Dabei geht es insbesondere um den Aspekt sicherer digitaler Identitäten, ohne deren erfolgreiche Implementierung als Fundament der Plattform ein solches Projekt zum Scheitern verurteilt wäre.

Ausgehend von den oben ausgeführten Vorüberlegungen legt die nachfolgende Untersuchung dar, dass eine erfolgreiche digitale Transformation der Verwaltung in Deutschland in erster Linie davon abhängen wird, ob an die bereits vorhandenen Strukturen angeknüpft werden kann. Eine disruptive Einführung gänzlich neuer Abläufe ist zu vermeiden, sinnvoller erscheint vielmehr ein behutsames und schrittweises Vorgehen, das die Belange möglichst vieler Interessenvertreter und Verantwortlicher von Beginn an in die Planungen einbezieht – das gilt nicht zuletzt für die Routinen und legitimen Befindlichkeiten der Beschäftigten in der Verwaltung selbst. Nur so kann der unbedingt notwendige Aufbau interner Expertise in digitalen Fragen gelingen.

Zudem muss beim Aufbau der digitalen Verwaltungsinfrastruktur bei jedem Schritt der bürgerzentrierte Ansatz mitgedacht werden. Entscheidend ist, wie die Bürger die digital angebotenen Dienstleistungen wahrnehmen, ob sie diese intuitiv nutzen können und ob sie ihnen vertrauenswürdig erscheinen. Die Befürchtungen beim Datenschutz sind ernst zu nehmen. Daher müssen die Bürger die Hoheit über ihre eigenen personenbezogenen Daten behalten. Über das Bürgerportal erteilen und entziehen sie selbst Zugriffsmöglichkeiten.

Mit diesem Ansatz unmittelbar verknüpft ist der Aspekt der Datensicherheit. Eine den höchsten Standards genügende Sicherheitsarchitektur ist essentiell für den Erfolg des Vorhabens. Nichts würde das Vertrauen der Bürger in den digitalen Staat mehr und nachhaltiger erschüttern als eine Verletzung der Datensicherheit in diesem Bereich, möglicherweise gar durch ausländische staatliche Akteure. Kernstück einer solchen hinreichenden Sicherheitsarchitektur und damit zugleich Fundament des E-Governments ist die Erschaffung einer sicheren digitalen Identität, die dem Bürger bei digitalen Verwaltungsdiensten als nicht korrumpierbares, stabiles Alter Ego dient. Die Anforderungen an eine solche digitale Identität insbesondere aus technischer Hinsicht bilden daher einen Schwerpunkt der Studie.

1.7 Die Leitfragen

Die Untersuchung orientiert sich an folgenden Leitfragen, die sich aus den Vorüberlegungen ergeben:

- Was ist die Zielsetzung der digitalen Transformation der Verwaltung?
- Wie kann das Vorhaben technisch sinnvoll umgesetzt werden?
- Welche Akteure sollen das Vorhaben umsetzen?
- Welche nichttechnischen Herausforderungen gibt es bei einem solchen Vorhaben?

1.8 Der Aufbau des Papiers

Das nachfolgende zweite Kapitel beschreibt, wie E-Government in naher Zukunft in Deutschland idealerweise aussehen könnte. Anhand konkreter narrativer Szenarien werden dabei die Bedeutung und der Nutzen von E-Government für verschiedene Bevölkerungsgruppen aufgezeigt. Dabei wird auch auf die Perspektive der Verwaltung eingegangen. Die zentralen Merkmale der umzusetzenden Infrastruktur werden anschaulich gemacht.

Im dritten Kapitel wird das Narrativ in die Vorhaben der Bundesregierung bei der digitalen Transformation der Verwaltung eingebettet. Zusätzlich zu einigen begrifflichen Erläuterungen werden die grundsätzlichen Überlegungen eingeführt, auf denen der folgende analytische Teil der Studie beruht. Diese Prämissen betreffen die Ziele der Maßnahmen sowie die Vorgehensweise der schrittweisen Umsetzung. Eingegangen wird zudem auf den Status quo der Vorhaben.

Im vierten Kapitel wird ausführlich diskutiert, welche Akteure geeignet erscheinen, das Vorhaben umzusetzen.

Die konkrete technische Umsetzung der Infrastruktur einschließlich der Frage sicherer digitaler Identitäten ist Gegenstand des fünften Kapitels. Die verschiedenen Optionen werden erörtert und abgewogen – mit dem Ziel, ein möglichst sicheres und benutzerfreundliches Modell zu finden, das von den Bürgern und den Akteuren innerhalb der Verwaltung angenommen wird.

Im sechsten Kapitel geht es um die weiteren Voraussetzungen und Parameter des Aufbaus von E-Government-Strukturen in Deutschland. Dies betrifft im Einzelnen die rechtlichen, politischen, gesellschaftlichen und ethischen Herausforderungen, die während der Umsetzung eines derart komplexen und anspruchsvollen Projekts beachtet werden müssen.

Das siebte Kapitel geht auf übergreifende Risiken der digitalen Transformation ein; im achten Kapitel werden Schlussfolgerungen aus den vorherigen Betrachtungen gezogen.

2 DAS SZENARIO: E-GOVERNMENT IN DEUTSCHLAND IM JAHR 2020

Wir befinden uns in nächster Zukunft. Familie Müller ist kürzlich von Köln nach Gummersbach umgezogen, weil Frau Müller dort eine neue Stelle als Grundschullehrerin angenommen hat. Vieles ist zu organisieren: Die neue Adresse muss angemeldet, das Auto der Familie umgemeldet werden. Für die beiden Töchter Sarah und Pinar, neun und sechzehn Jahre alt, müssen eine neue Grundschule und ein neues Gymnasium gefunden werden. Ungern erinnern sich Frau und Herr Müller daran zurück, als sie 2011 von Essen nach Köln gezogen sind. Monatelang gab es keine freien Termine bei den Ämtern – und die schließlich verfügbaren Termine lagen so unglücklich, dass jeweils einer von beiden einen Tag Urlaub nehmen musste.

Ein solcher Aufwand gehört inzwischen zum Glück der Vergangenheit an. Kurz nach dem Einzug melden sich die Müllers einfach auf dem Bürgerportal an, für das sie sich direkt nach dem Start der neuen digitalen Verwaltungsservices im vergangenen Jahr registriert hatten. Eine einfache Anmeldung genügt, und alle notwendigen Dienstleistungen der örtlichen Verwaltung sind mit wenigen Klicks verfügbar. Für die Anmeldung benötigt man lediglich einen elektronischen Personalausweis, der nur an das an den heimischen PC angeschlossene Lesegerät gehalten werden muss.

Dank der sehr übersichtlichen Benutzeroberfläche kann das Bürgerportal intuitiv bedient werden. Frau Müller schätzt zudem die Infokästen, die mittels Algorithmen generiert werden: Sie erscheinen automatisch auf dem Bildschirm, um situationsabhängig darauf hinzuweisen, welche Dokumente noch fehlen oder welche Schritte für einen bestimmten Vorgang noch abgeschlossen werden müssen.

Über das Portal gelangen die Müllers schnell zu den Seiten der Schulbehörde, die ausführlich über die nächstgelegenen Schulen in ihrem Bezirk informieren. Die Anmeldung ihrer Töchter ist online schnell erledigt. Auch die Anmeldung des neuen Wohnsitzes und die Ummeldung des Autos klappen problemlos. Herr Müller kümmert sich gleich noch um einen Anwohnerparkausweis. Die fällige Jahresgebühr von 30 Euro kann er ebenfalls gleich online mittels eines Bezahldienstes leisten, der im Bürgerportal integriert ist. Ein Aufkleber

für sein Auto, der die Parkberechtigung bestätigt, ist nicht mehr nötig; die Daten können vorbeikommende Angestellte des Ordnungsamts problemlos mit ihren Geräten anhand des Fahrzeugkennzeichens abgleichen.

Der Wagen soll ohnehin nur vorübergehend auf der Straße parken. Die Müllers wollen an ihrem Einfamilienhaus eine großzügige Garage bauen. Für die Baugenehmigung genügt es, über das Bürgerportal einen Antrag zu stellen. Die dafür nötigen Baupläne können die Eheleute bequem online hochladen und an das Bauamt übermitteln. Da Herr Müller bei einer Bank in Bonn arbeitet und entsprechend viel Zeit mit Pendeln verbringt, erledigt er dies, indem er mit einer App auf seinem Smartphone auf das Bürgerportal zugreift, während er im Regionalexpress sitzt. Sogar wichtige Dokumente kann er dort elektronisch signieren.

Währenddessen sucht Pinar nach einem Praktikumsplatz in den kommenden Sommerferien. Die Bewerbung ist durch das Bürgerportal einfacher geworden. Sie meldet sich über ihren eigenen Account auf dem Portal an, indem sie sich mit ihrem Smartphone identifiziert. Über das Portal hat sie Zugriff auf einen Online-Speicher, auf dem private Dokumente hinterlegt sind. Dort findet sie auch ihre aktuellen Schulzeugnisse, die sie nur noch herunterladen und ihrer Bewerbung beifügen muss.

Auch Frau Dr. Schmidt ist inzwischen sehr glücklich über das digitale Bürgerportal. Viele Dinge sind für die Rentnerin, die in Ingolstadt lebt, seitdem leichter geworden. Als sie zum ersten Mal in ihrer Tageszeitung von der Möglichkeit erfuhr, all ihre Verwaltungsangelegenheiten künftig „im Internet" zu erledigen, war sie zunächst verunsichert, zugleich jedoch neugierig. Sie meldete sich für einen der kostenlosen Kurse an, die von der Stadt angeboten wurden, um die Bürger mit der Nutzung des Portals vertraut zu machen. Die Erklärungen waren leicht verständlich; schnell lernte Frau Dr. Schmidt mit dem digitalen Verwaltungsportal umzugehen. Rentenangelegenheiten erledigt sie inzwischen schnell und einfach online. Mit der digitalen Identität, die sie zu diesem Zweck eingerichtet hat, kann sie sich auf der Webseite ihrer Krankenkasse anmelden, um dort Mitgliedsbescheinigungen herunterzuladen oder Behandlungen zu beantragen.

Über das Bürgerportal konnte sie zudem ihren Schwerbehindertenausweis beantragen, da sie seit einigen Monaten auf einen Rollstuhl angewiesen ist. Für diesen Vorgang musste sie dem zuständigen „Zentrum Bayern Familie und Soziales" Unterlagen ihres Hausarztes übermitteln, die ihre Gesundheitsdaten enthielten. Dafür musste Frau Dr. Schmidt sich zur zusätzlichen Absicherung der Identifizierung mit ihrem Fingerabdruck anmelden. Auch das war dank des Scanners, der ihr vom Amt kostenlos zur Verfügung gestellt wurde, kein größeres Problem. Sie ist zwar von den Vorteilen des Bürgerportals inzwischen überzeugt und nutzt es häufig – dennoch lässt sie sich manchmal zum Amt fahren, um ihre Angelegenheiten vor Ort zu erledigen. Seitdem die Verwaltungsangestellten durch das neue Online-System bei der täglichen Arbeit entlastet wurden, können Bürger viel schneller Termine bekommen. Frau Dr. Schmidt ist trotz allem Komfortgewinn sehr froh darüber, dass sie weiterhin persönlich mit den Angestellten

in der Verwaltung sprechen kann und auch kein Druck ausgeübt wird, die Interaktionen auf die virtuelle Welt zu beschränken.

Vor fast zwei Jahren ist Samira Mansour aus Syrien nach Deutschland geflohen, um dem Bürgerkrieg in ihrem Land zu entkommen. Gerade weil hier vieles neu und unvertraut war, war Frau Mansour froh darüber, dass sie den Stand ihres Asylverfahrens stets online nachverfolgen konnte und kann. Registrierung und Anmeldung waren denkbar einfach: Denn schon mit ihrer Aufenthaltsgestattung – die sie ausgehändigt bekommen hatte, um sich während des laufenden Verfahrens ausweisen zu können – kann sie sich leicht elektronisch auf der E-Government-Plattform identifizieren. Selbstverständlich geht das auch mit ihrem elektronischen Aufenthaltstitel, den sie als anerkannte Geflüchtete mittlerweile stets bei sich trägt. Obwohl sie sich so schnell wie möglich über das Bürgerportal zu staatlich geförderten Deutsch- und Integrationskursen angemeldet hatte und schnell Fortschritte machte, ist sie froh, dass die Erklärungen und Hilfen auf dem Portal in vielen Sprachen angeboten werden, unter anderem auf Englisch und Arabisch.

Nach den Strapazen der Flucht und den Unsicherheiten des Asylverfahrens fühlt sich Frau Mansour nun endlich bereit, ihre Zukunft in Hamburg zu planen. Schon seit dem Abschluss ihres Informatikstudiums in Aleppo hat sie Ideen für ein Start-up, die sie nun umsetzt. Die notwendige Anmeldung ihrer selbstständigen Tätigkeit erledigt sie bequem über das Bürgerportal. Notwendige Informationen dafür sind auf ihrem Nutzerkonto hinterlegt: der Abschluss und positive Bescheid ihres Asylverfahrens und die entsprechende Erlaubnis, uneingeschränkt in Deutschland zu arbeiten. Sie muss die entsprechenden Daten nur den zuständigen Behörden wie dem Finanzamt Altona gegenüber freischalten, damit diese sie für den angefragten Verwaltungsvorgang einsehen und verifizieren können.

Seit seiner Scheidung vor drei Jahren ist Martin Krause alleinerziehender Vater seines inzwischen fünfjährigen Sohns. Es fällt ihm nicht leicht, seine Arbeit in einer Werbeagentur und die Erziehung unter einen Hut zu bringen. Da ist es eine große Erleichterung, dass er inzwischen über das Bürgerportal viele Angelegenheiten nach Feierabend von zu Hause aus erledigen kann. Dabei war er bei der Einführung des Portals noch skeptisch gewesen. Vor allem die Sicherheit und der Schutz seiner persönlichen Daten machten ihm große Sorgen. Konnte er sich wirklich sicher sein, dass nur diejenigen Zugriff bekommen, die dazu auch berechtigt sind?

Nach eingehender Beschäftigung mit der Plattform ist er vom Schutzkonzept überzeugt. Besonders angetan ist er von dem Umstand, dass er die Kontrolle über die sensiblen Daten behält und er den Behörden die Berechtigung erteilt, seine Daten einzusehen – falls diese nicht ohnehin in den bestehenden Registern des Staats liegen – und zu nutzen. Ist der Vorgang abgeschlossen, kann er bequem die Berechtigungen entziehen, so dass ein weitergehender Zugriff tatsächlich ausgeschlossen ist. Er weiß um sein Recht – solange und soweit nicht im Einzelfall gesetzliche Grundlagen dem entgegenstehen, andere verbindlich auffordern zu dürfen, über ihn gespeicherte Informationen zu löschen. Er ist sehr zufrieden mit der auf dem Bürgerportal gefundenen Lösung,

dieses Recht umzusetzen. Wichtig ist ihm zudem, dass er auf einer gut strukturierten Übersichtsseite jederzeit nachvollziehen kann, welcher Akteur zu welchem Zeitpunkt und zu welchem Zweck Zugriff auf welche seiner Daten bekommen hat. Herr Krause hat das Gefühl und die Sicherheit, tatsächlich die volle Kontrolle über Bereitstellung und Verwendung seiner persönlichen Daten zu besitzen.

Auch die Sicherheitsarchitektur sagt Herrn Krause zu. Als er kürzlich eine Änderung seines Kindergeldbescheids beantragen wollte, musste er zusätzlich zu seiner Anmeldung beim Portal per Personalausweis eine sechsstellige PIN eingeben. Hingegen brauchte er die PIN nicht, als er eine Woche später den jungen Golden Retriever, den er seinem Sohn zum Geburtstag geschenkt hatte, zur Hundesteuer anmeldete. Von dieser sinnvollen Sicherheitsabstufung je nach Sensibilität des Verwaltungsvorgangs ist er beeindruckt.

Seit mittlerweile zwei Jahrzehnten ist Frau Stokowski in der Verwaltung der Stadt Cottbus tätig, aber so zufriedenstellend wie seit Einführung der neuen E-Government-Infrastruktur empfand sie ihre Arbeit bislang noch nicht. Viele sich stets wiederholende Routineaufgaben übernimmt inzwischen eine intelligente Software und zahlreiche Verwaltungsvorgänge lassen sich jetzt wesentlich effizienter gestalten. Zwar war ein Großteil der Belegschaft zu Beginn noch verunsichert. Jedoch haben die vielen guten Fortbildungen dazu beigetragen, dass sich die Mitarbeiter in der digitalen Transformation der Verwaltung inzwischen wohlfühlen. Von Anfang an wurden ihre Sorgen und Bedenken ernst genommen und es wurde über jeden Erneuerungsschritt gut informiert.

Um die neuen digitalen Systeme mit aufzusetzen, laufend zu testen und ihre Funktionalitäten bei Bedarf dynamisch weiterzuentwickeln, wurden neue IT-Experten eingestellt. Sie haben sich sehr gut in die bestehende Belegschaft eingefügt.

Die Angestellten haben in interdisziplinären Workshops gemeinsam entwickelt, was sie heute im Verwaltungsalltag an Technik und Anwendungen nutzen. Der Fokus der täglichen Arbeit liegt jetzt mehr darauf, die Bürger bei ihren Anliegen ausführlich und eingehend zu beraten – per E-Mail, im Online-Chat und persönlich vor Ort.

3 GRUNDSATZENTSCHEIDUNGEN DER TECHNOLOGIE-ENTWICKLUNG UND TRANSFORMATIONSORGANISATION

So wie im zweiten Kapitel beschrieben, könnte eine digitale Verwaltungsstruktur in Deutschland zukünftig aussehen. Doch bis dahin ist es noch ein weiter Weg. Denn die Digitalisierung ist ein komplexer Transformationsprozess. Die Vielschichtigkeit der Umstände, bereits gewachsene Strukturen, die Unumgänglichkeit von steten Änderungen und Anpassungen im Laufe des Projekts sind zu berücksichtigen. Darüber hinaus müssen alle Beteiligten durch Überzeugungsarbeit, Weiterbildung und Ausbildung mitgenommen werden. All diese Faktoren sind immanenter Teil der Digitalisierung. Sie sollten auch als solche begrüßt, akzeptiert und eingeplant werden – und nicht als Hemmnis oder Bremse verstanden werden. Visionen und Digitalisierungsprojekte, die diese Erfahrungen sowie die Natur einer solchen Transformation ignorieren, werden scheitern.

Bei der Umsetzung umfangreicher Digitalisierungsprojekte stellt sich zusätzlich zur Frage nach der richtigen Technologie, die eingesetzt werden soll, auch die nach dem geeigneten nichttechnischen Rahmen, der richtigen Projektplanung und – als erster Schritt – die Frage nach der richtigen und präzisen Zielsetzung.

Hier ist als Ausgangspunkt entscheidend, die Digitalisierung der Verwaltungsstrukturen nicht bloß als ihre Entmaterialisierung zu begreifen. Es geht nicht darum, den alten Offline-Zustand lediglich online zu reproduzieren. Gerade in der Verwaltung sind viele Strukturen historisch gewachsen und haben sich im Verlauf der Jahrzehnte den jeweiligen Gegebenheiten soweit notwendig und möglich angepasst. Bevor mit der digitalen Transformation begonnen wird, ist deshalb zu untersuchen, ob und inwieweit die vorhandenen Architekturen noch sinnvoll sind. Dies ist eine der entscheidenden Chancen eines Digitalisierungsprojekts: die Möglichkeit, ganz neu zu denken und neu zu gestalten. Werden Unzulänglichkeiten in den alten Strukturen identifiziert, dann sollten sie natürlich nicht beim digitalen Neuaufbau übernommen werden. Eine digitale Transformation ist gerade kein Selbstzweck: Erstens sollen die Dienst- und Arbeitsbedingungen in den Verwaltungen verbessert werden. Zweitens sollen Bürger einfacher Verwaltungsangelegenheiten erledigen können.

Ein Beispiel aus Österreich kann dies veranschaulichen.[33] Mit dem gemeinsamen Projekt „Antraglose Familienbeihilfe" (ALF) des Bundesministeriums für Finanzen und des Bundesministeriums für Familien und Jugend erhalten Familien anlässlich der Geburt eines Kinds automatisch die Familienbeihilfe,[34] ohne ein weiteres Formular ausfüllen zu müssen. Es genügt, dass sich die Eltern im Krankenhaus bei der Geburt ihres Kinds mit ihrem Personalausweis identifizieren. Das Krankenhaus selbst meldet die Geburt des Kinds dem Standesamt, das die Daten an die Finanzverwaltung weiterleitet. Dort wird der Anspruch auf Familienbeihilfe automatisiert verarbeitet und die Leistung vollzogen.[35]

33 Siehe *https://www.bmf.gv.at/egovernment/projekte/e-gov-projekte.html.*

34 Die Familienbeihilfe entspricht in etwa dem Kindergeld in Deutschland.

35 Bertelsmann Stiftung 2017, S. 19 f.

Insgesamt profitieren von dieser Lösung rund 80.000 Familien pro Jahr. Hier wurden im Zuge der Digitalisierung einige unnötige Schritte abgeschafft (Terminfindung beim Amt, Ausfüllen von entsprechenden Formularen, die Bearbeitung der Formulare durch die Mitarbeiter, die Ausstellung einer Antwort), statt Schritt für Schritt sämtliche Maßnahmen ins Digitale zu übersetzen.

Falsch umgesetzt – sei es mangels ausreichender Planung oder wegen Fehlern bei der technischen Implementierung – kann eine digitale Transformation allerdings schnell schaden, zum Beispiel bei einer nicht abgestuften und unsicheren Freigabe sensibler Daten der Bürger. Auch deshalb bedarf es immer einer gesamtheitlichen Herangehensweise unter realistischer Betrachtung der aktuellen Gegebenheiten. Eine von Beginn an eingeplante Begleitforschung kann ebenfalls helfen, neue Lösungswege aufzuzeigen, neue Bedarfe zu ermitteln und die Auswirkungen der Transformation unabhängig zu verifizieren.

3.1 Zielsetzung von E-Government-Maßnahmen

Das Kompetenzzentrum Öffentliche IT kam 2015 in einem Gutachten zu dem Schluss, dass sich E-Government in Deutschland bislang im Kreis drehe und nicht vorankomme: Geringes Angebot, ungenügende Benutzerfreundlichkeit und fehlender Mehrwert der elektronischen Verwaltungsverfahren führten dazu, dass bestehende Angebote durch die Bürger kaum genutzt werden. Seit einigen Jahren sei die Inanspruchnahme sogar tendenziell rückläufig. Fehlende Nutzerzahlen wiederum führten dazu, dass erhoffte Effizienzgewinne ausblieben und E-Government für die Verwaltung nicht zu Entlastungen führe, sondern eher zum zusätzlichen Kostenfaktor werde.[36]

Ziel von E-Government sollte die Bewältigung des digitalen Wandels als Ganzes sein, und nicht, einzelne Abläufe innerhalb der Verwaltung zu optimieren. Es sollten deshalb nicht einfach öffentliche Dienstleistungen verbessert, sondern bestehende Prozesse einer grundlegenden Revision unterzogen werden.

Mit anderen Worten: Es kann gerade nicht darum gehen, bloß den Status quo online zu stellen. Ziel ist eine schrittweise echte Modernisierung der Verwaltung.[37] Dabei sind ein Online-Zugang für Bürger und der Umgang mit ihren digital verfügbaren Daten lediglich zwei Bausteine.

3.2 Vorgehen und Priorisierung

Eine nachhaltige Modernisierung sollte anstreben, Defizite in der Verwaltungspraxis abzubauen, insbesondere Redundanzen.

36 Jens Fromm et al., E-Government in Deutschland: Vom Abstieg zum Aufstieg, 2015, ÖFIT-Whitepaper auf der Grundlage des Gutachtens „Bürokratieabbau durch Digitalisierung: Kosten und Nutzen von E-Government für Bürger und Verwaltung" im Auftrag des Nationalen Normenkontrollrats. Berlin: Kompetenzzentrum Öffentliche IT und Nationaler Normenkontrollrat. S. 5.

37 So im Ergebnis auch das Bundesministerium des Innern, für Bau und Heimat, Referat 02, auf S. 2 „Stand und Perspektiven des E-Governments in Deutschland" im „Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften", 2016.

Verbesserungen sind in den folgenden Bereichen möglich:

- Lange Wartezeiten auf einen Behördentermin, insbesondere in Ballungsgebieten und Großstädten
- Unzureichende Versorgungsinfrastruktur gerade bei Verwaltungsdienstleistungen in vielen ländlichen Gebieten aufgrund von Schließungen und Zusammenlegungen infolge des Strukturwandels
- Verstreute Angebote und unübersichtliche Verwaltungsdienstleistungen
- Teilweise schwerverständliche Behördensprache im Umgang mit Bürgern; leicht verständliche Sprache sowie gute Anleitung und Auffindbarkeit sind der Schlüssel für die Akzeptanz des Verwaltungshandelns; angesichts signifikanter Migration nach Deutschland ist auch die Nutzung weiterer Sprachen zu erwägen
- Redundanzen im Hinblick auf die wiederholte An- und Eingabe derselben Daten durch Bürger, was auch zu Zeitverlusten führt – daher Hinwendung zum „Once only"-Prinzip[38]
- Redundanzen bei der Ablage und Speicherung von Daten: In Deutschland gibt es mehr als 200 unterschiedliche Register,[39] von den dezentralen Registern für die innere Verwaltung (Melde-, Personenstands- oder Personalausweisregister) bis hin zu Registern für Migration, Datenbanken der Sicherheitsbehörden oder Statistikregistern. Die Daten der Bürger liegen entsprechend dezentral und verteilt und teilweise redundant in unterschiedlichen Datenbanken. Bei der Frage nach der Zusammenlegung von Registern ist danach zu entscheiden, wo der Bedarf besonders hoch ist.[40]
- Bislang zu geringe Standardisierung der Daten; diese sollten zentral mit einem einzigen Schritt geändert oder gelöscht werden können, so dass technisch diese Daten an allen weiteren Stellen simultan angepasst werden; dies ließe sich bei hinreichender Standardisierung und Kompatibilität auch durch den Einsatz entsprechender Infrastrukturen umsetzen
- Mehr elektronische Partizipation, wie im Koalitionsvertrag angedacht[41]
- Verbesserung nachhaltigen Behördenhandelns: durch Digitalisierung geringerer Papierverbrauch innerhalb der Behörde und weniger Individualverkehr zur Behörde
- Bislang zu geringe Akzeptanz des elektronischen Personalausweises; Etablierung als universelles, sicheres und mobil einsetzbares Authentifizierungsmedium, das zugleich benutzerfreundlich ist[42]
- Verbesserung der digitalen Souveränität der Bürger und erhöhte Transparenz des Verwaltungshandelns: Anhand eines entsprechend eingerichteten Bürgerkontos könnten Bürger einsehen, welche Daten beim Staat vorliegen und welche Behörde darauf Zugriff genommen hat; über das Konto müssten sie – im Rahmen der rechtlichen Vorgaben und der Notwendigkeiten für den jeweiligen Verwaltungsvorgang – den Umgang mit ihren persönlichen Daten steuern können[43]
- Erhöhte Nachvollziehbarkeit des bürgerbezogenen Verwaltungshandelns durch automatische und einsehbare Dokumentation

38 „Once only"-Prinzip, das es Behörden ermöglicht, Daten über gemeinsame Register und eindeutige, übergreifende Identifikationen zu verknüpfen und somit auch die Mehrfacheinreichung von Dokumenten durch Bürger zu reduzieren. Bürger sollen ihre Daten grundsätzlich nur einmal eingeben müssen. Mit ihrer Zustimmung sollen bestimmte zur Verfügung gestellte Daten unter den Behörden weitergegeben werden, berechtigte Leistungsansprüche sollen antragslos und proaktiv gewährt werden können.

39 Registerlandschaft aufgeschlüsselt in: Nationaler Normenkontrollrat (Hg.), Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, Oktober 2017, *https://www.normenkontrollrat.bund.de/resource/blob/72494/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-downloadnkr-gutachten-2017-data.pdf?download=1*, S. 14 ff., 23 ff.

40 Ebd., S. 20: Zu den Top 5 der Register nach Nutzung für behördliche Dienstleistungen für Bürger gehören der Reihe nach: das örtliche Melderegister, das zentrale Fahrzeugregister, das Handelsregister, das Gewerberegister, das örtliche Personenstandsregister. S. 52: Der Ruf nach einem Registermodernisierungsgesetz ist vermehrt zu hören.

41 Koalitionsvertrag 2018, S. 46.

42 Ebd.

43 Ebd., S. 45.

3.3 Von anderen Ländern lernen, aber deutsche Gegebenheiten beachten

Die föderale Struktur der Bundesrepublik ist eine der zentralen Herausforderungen für die Umsetzung von E-Government-Projekten. Es ist eine gewachsene heterogene Struktur,die regionale Unterschiede zulässt und verfestigt. Zudem ist sie grundgesetzlich und tief in den kulturellen Vorstellungen der Bürger verankert. Schon deshalb fällt ein Vergleich mit vielen anderen europäischen Ländern schwer, die E-Government-Strukturen bereits erfolgreich eingeführt haben. Dies zeigt ein Blick auf das gern zitierte Vorzeigebeispiel: Estland.

Estland und Deutschland haben grundlegend unterschiedliche staatsorganisatorische Strukturen. Hinzu kommen sehr verschiedene Ausgangsbedingungen, die eine Vergleichbarkeit schwierig machen. Estland gibt es als unabhängigen Staat in seiner jetzigen Gestalt erst seit seiner Abspaltung von der Sowjetunion im Jahr 1991. Dieses Ereignis war eine radikale Zäsur, die ein komplettes Neudenken für den Aufbau von Verwaltungsstrukturen nötig machte. Mit der in den 90er-Jahren aufkommenden Digitalisierung schuf dies ideale Voraussetzungen für eine umfassende E-Government-Architektur. Diese Situation ist nicht mit den jahrzehntelang gewachsenen Verwaltungsstrukturen in Deutschland und den Ländern der Bundesrepublik zu vergleichen. Zudem sind die Unterschiede in den jeweiligen Registerstrukturen beachtlich: In Estland liegen sämtliche Daten der Bürger in einer einzigen zentralen Datenbank. Dies ist in der Bundesrepublik bislang völlig anders und viel komplexer organisiert. Zudem haben kleinere Länder gegenüber größeren generell den Vorteil, einmal eingeführte Systeme bei Fehlentwicklungen deutlich einfacher und schneller anpassen oder ersetzen zu können.

Schon deshalb muss für Deutschland ein eigener, an die hiesigen Verhältnisse und Gegebenheiten sorgfältig angepasster Ansatz gefunden werden. Das heißt selbstverständlich nicht, dass bei der Konzipierung des E-Governments nicht von anderen Ländern gelernt werden sollte, insoweit etablierte Beispiele hierzulande realistisch umgesetzt werden können.

3.4 Schrittweise digitale Transformation

Obwohl sich die vorliegende Studie für einen grundlegend neuen, umfassenden Ansatz bei der digitalen Transformation der Verwaltung ausspricht, sollte die Umsetzung des Vorhabens keinesfalls überstürzt und vorschnell angegangen werden. Damit ein Projekt wie die Etablierung nachhaltiger und funktionierender E-Government-Strukturen in Deutschland gelingen kann, müssen unter anderem die Eigenheiten einzelner Behörden und anderer staatlicher Organisationen beachtet werden. Zudem müssen insbesondere bereits bestehende, gut funktionierende Online-Systeme des Bundes, einzelner Bundesländer und der Kommunen sowie der jeweilige Digitalisierungsgrad der einzelnen Stellen in Planung und Umsetzung von Beginn an einbezogen werden.

Ein solches iteratives, also schrittweises und sich wiederholendes Vorgehen ist ein Gegenmodell zu einer disruptiven Einführung des E-Governments. Ein zu großer,

plötzlicher Umbruch liefe Gefahr, in der Verwaltung abgelehnt und von Bürgern nur bedingt angenommen zu werden. Gerade innerhalb der Verwaltung ist bei einer Einführung, die schrittweise erfolgt und als organisch empfunden wird, weil sie an gegebene und bewährte Strukturen anknüpft, eine deutlich höhere Akzeptanz zu erwarten. Zusätzlich erforderliche Qualifikationen und Kompetenzen im Umgang mit E-Government-Architekturen können dabei durch Trainings und Fortbildungen begleitend zu den normalen Behördenabläufen gefördert und schrittweise aufgebaut werden.

Ein weiterer Vorteil dieser Vorgehensweise: Auch eventuelle Schwierigkeiten oder Streitfälle müssen nicht vorher vollständig antizipiert und geklärt werden, sondern können im Verlauf der Umsetzung angegangen und gelöst werden. So kann zunächst dahingestellt bleiben, ob eine länderübergreifende Zusammenlegung von Teilbereichen oder eine Teilharmonisierung der Registerlandschaft in Deutschland erfolgen soll. Diese Punkte sind zum Teil im politischen Raum sehr strittig. Müsste man die Entscheidung zu diesen Fragen vorab klären, wären beträchtliche und kaum vertretbare Verzögerungen zu erwarten. Bei dem hier vorgestellten Ansatz iterativer Vorgehensweise ergeben sich Lösungen für Teilaspekte im Laufe des Transformationsprozesses und können dann umgesetzt werden, wenn dies wirklich notwendig wird. Andere Teile des Vorhabens bleiben davon unberührt.

3.5 Orientierung an Best Practices und erfolgreichen Modellen

Es erscheint unbedingt empfehlenswert, beim Aufbau einer E-Government-Architektur möglichst viel aus den Erfahrungen der Privatwirtschaft, den international erfolgreichen Umsetzungen von Digitalisierungsprojekten und der Entwicklung digitaler Güter und Services zu lernen.[44]

Eine Anwendung von Best Practices aus der Privatwirtschaft bei Unternehmen, die komplexe digitale Dienstleistungen anbieten, erscheint insbesondere in folgenden Punkten sinnvoll:

- Herausarbeiten und Priorisieren der Bedarfe der Bürger. Es gibt bereits viele Erhebungen dazu (siehe oben), diese sollten angereichert werden mit regelmäßigen Feedbackschleifen mit den Nutzern sowie der anonymen Auswertung und Analyse der tatsächlichen Nutzung zur Optimierung des digitalen Produkts. Kapazitätsengpässe sollten dabei zuerst angegangen werden.
- Anknüpfen der neuen Infrastruktur an bereits funktionierende Systeme und Ergänzungen. Ein Beispiel wären die bereits heute gut funktionierenden Online-Modelle in der Verwaltung der nordrhein-westfälischen Landeshauptstadt Düsseldorf. Auf diese Weise werden die Neuerungen auch eher behördenintern akzeptiert, da so auch die bisher erfolgreichen Umsetzungen wertgeschätzt werden.
- Die „User Journey" genau analysieren und als Einheit erkennen. Mit User Journey sind alle Schritte gemeint, die ein Nutzer im interaktiven System geht, um sein jeweiliges Ziel zu erreichen (unter Einbeziehung aller Entscheidungspunkte), sowie die Erfahrungen, die er dabei macht. Das gesamte Nutzererlebnis in der digitalen Verwaltung ist von Anfang bis Ende zu durchdenken. Es reicht nicht aus, wenn zwar der Einstieg leichtfällt, die Nutzerfreundlichkeit anschließend aber abnimmt.

44 Zu diesem Ergebnis kommt auch der U.S. Digital Service, der in einem „Playbook" die wichtigsten 13 Prinzipien zusammengefasst hat (*https://playbook.cio.gov/*).

- Einfache und intuitive Gestaltung der Online-Infrastruktur („Usability"). Die Benutzeroberfläche muss für die meisten Nutzer selbsterklärend und leicht zu bedienen sein. Nur dann ist die Nutzungsbarriere so niedrig wie möglich.

Insbesondere eine bürgerzentrierte Herangehensweise ist für die Akzeptanz und den Erfolg der Verwaltungsdigitalisierung unerlässlich. Der Fokus auf den Bürger spiegelt sich im Koalitionsvertrag, der die Einführung eines Bürgerkontos vorsieht:

„Wir werden in einem digitalen Portal für Bürgerinnen und Bürger sowie für Unternehmen einen einfachen, sicheren und auch mobilen Zugang zu allen Verwaltungsdienstleistungen ermöglichen. Dazu vernetzen wir geeignete zentrale und dezentrale Verwaltungsportale in einem Portalverbund. In dem damit verknüpften Bürgerkonto hat der Bürger Einblick, welche Daten beim Staat vorliegen, welche Behörde darauf Zugriff genommen hat und kann den Umgang mit seinen persönlichen Daten steuern."[45]

45 Koalitionsvertrag 2018, S. 45.

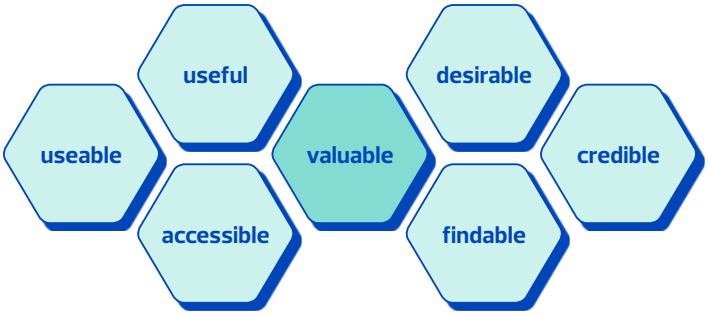
Im Mittelpunkt der nutzerzentrierten Entwicklung digitaler Verwaltungsdienste steht die Nutzerfreundlichkeit der digitalen Produkte und Dienste. Die einfache Nutzung begründet den massiven Erfolg einiger weniger großer Plattformanbieter, die sich insbesondere aus diesem Grund gegenüber Wettbewerbern durchgesetzt haben. Das ambitionierteste, sicherste Angebot wird sich nicht verbreiten, wenn die Benutzeroberfläche schwer zu bedienen ist und den Nutzer überfordert.

Den mangelnden Fortschritt beim Ausbau von E-Government führen öffentliche Stellen in Deutschland oft auf das fehlende Interesse der Bürger zurück.[46] Als Grund nennen 80 Prozent derjenigen, die keine Leistungen des E-Governments in Anspruch nehmen, dass sie das derzeitige E-Government-Angebot schlichtweg nicht überzeugt.[47] Sie bevorzugen weiterhin den persönlichen Kontakt zur Verwaltung, die bislang angebotenen Online-Services erscheinen ihnen zu umständlich und kompliziert.

46 Katrin Suder, „Digitaler Glanz ist noch kein Gold", Wirtschafts-Woche, 13. Dezember 2012, *https://bit.ly/2B79Qfo.*

47 Vgl. McKinsey, „E-Government in Deutschland: Eine Bürgerperspektive", 2014.

Angelehnt an die „Usability Honeycomb"[48] lässt sich der Aspekt der Nutzerfreundlichkeit veranschaulichen. Sie trägt die folgenden Faktoren als wesentlich für ein zufriedenstellendes Anwendungserlebnis zusammen:



48 Die UX-Honeycomb wurde von dem User-Experience-Experten Peter Morville entwickelt, vgl. Dane Wesolko, „Peter Morville's User Experience Honeycomb", 2016, *https://bit.ly/2uZrJHD.*

- Useful (nützlich): Es geht hier um das Bemühen, neue Lösungen nur für Probleme zu finden oder für verbesserungsbedürftige Bereiche. Die Bedarfe müssen dementsprechend zunächst ermittelt werden. Das Wissen sollte eingesetzt werden, um Lösungen zu definieren, die nützlicher sind als die zuvor.
- Useable (benutzbar): Die Benutzerfreundlichkeit ist unerlässlich. Daher braucht es zusätzlich zu einem sicheren und funktionierenden Backend eine ansprechende und leicht zu bedienende Nutzeroberfläche (Frontend).[49]
- Desirable (wünschenswert): Der Nutzer muss auch ohne langwieriges Einlesen und eigene Recherche klar erkennen können, wo der Nutzen der Plattform oder der digitalen Leistung ist. Dies gilt auch für Informationen innerhalb der Organisation des Anbieters: Dort sollten alle geschult und informiert sein und mit dem System umgehen können. Zudem sollten sie ebenfalls einen Nutzen sehen.
- Findable (auffindbar): Es sind gut navigierbare Webseiten und Services zu entwerfen, damit die Benutzer stets den Service finden, den sie brauchen.
- Accessible (zugänglich): Der Zugang zu den Diensten muss niedrigschwellig, barrierefrei und inklusiv sein.
- Credible (glaubwürdig): Hiermit ist gemeint, dass die Benutzer Vertrauen haben und glauben, was das System ihnen mitteilt.
- Valuable (mehrwertstiftend): Das Online-Portal muss einen Mehrwert bieten und zur Lösung beitragen, etwa dem Nutzer Zeit sparen oder neue Optionen bereitstellen.

49 „Die Begriffe Front-End und Back-End (von englisch für Vor- bzw. Über- und Unterbau, wörtlich vorderes und hinteres Ende) werden in der Informationstechnik an verschiedenen Stellen in Verbindung mit einer Schichteneinteilung verwendet. Dabei ist typischerweise das Front-End näher am Benutzer, das Back-End näher am System. In manchen Fällen ist diese Interpretation nicht anwendbar, es gilt aber prinzipiell, dass das Front-End näher an der Eingabe und das Back-End näher an der Verarbeitung ist" (*https://de.wikipedia.org/wiki/Front-End_und_Back-End*).

Die verschiedenen Punkte lassen sich in drei Folgerungen zusammenfassen:

1. **Konkrete Bedarfe feststellen:**
   valuable, *desirable* (also auch in Betracht ziehen, ob ein alternativer Zugang gewünscht bleibt); siehe oben „Priorisierung und Zielsetzung"
2. **Auf Benutzerfreundlichkeit achten:**
   useful, usable, findable
3. **Infrastruktur durch Staat zur Verfügung stellen:**
   Um *accessibility* zu gewährleisten im Rahmen einer bereits vorhandenen *credibility* (Vertrauen in den Staat)

3.6 Der Status quo

Die Bemühungen der Bundesregierung, die digitale Transformation der Verwaltung in der laufenden Legislaturperiode zu beschleunigen, sollten bereits bestehende Projekte im E-Government berücksichtigen. Das ausgewiesene Ziel bleibt, die Verwaltung flächendeckend zu digitalisieren und die bereits etablierten Verwaltungsportale

aller Ebenen – also Bund, Länder und Kommunen – in einem Portalverbund intelligent miteinander zu verknüpfen.

In dieser Hinsicht können einige Problembereiche identifiziert werden, die den Fortschritt in Deutschland bislang behindern. Auf verschiedenen Verwaltungsebenen werden bislang noch zu heterogene Leistungen angeboten, und zu wenige Lebens- und Geschäftslagen sind vollständig abgedeckt. Noch zu oft werden papierbasierte Anträge und Formulare für Verwaltungsvorgänge vorausgesetzt.

Ein Meilenstein hingegen ist das Inkrafttreten des Onlinezugangsverbesserungsgesetzes (oder Onlinezugangsgesetz, OZG) im August 2017. Es gibt ausdrücklich das Ziel aus, die digitale Transformation bis 2022 so weit vorangebracht zu haben, dass alle onlinefähigen Verwaltungsdienstleistungen über – mit dem Portalverbund verknüpfte – Verwaltungsportale angeboten und medienbruchfrei abgewickelt werden können. Im Oktober 2017 hatte der IT-Planungsrat die Grundprinzipien der Architektur dieses Verbunds und im Februar 2018 die Pilotierung eines Online-Gateways als technische Infrastruktur des Verbunds bis Herbst 2018 beschlossen. Es ist geplant, dass sich die Verwaltungsportale des Bundes und der Länder ab Ende 2018 am Portalverbund anbinden können. Hinzu kommen die Services der Kommunen, die über die Portale der Länder ebenfalls mit dem Verbund verknüpft werden sollen.

4 AKTEURE DER UMSETZUNG

Eine maßgebliche Entscheidung gleich zu Beginn von Digitalisierungsprojekten ist die Frage, ob ein so komplexes Projekt wie die umfassende Einführung von E-Government-Strukturen intern oder extern realisiert werden soll. Also: Sollte der Staat diese Aufgabe selbst übernehmen oder delegieren?

Grundsätzlich sind unterschiedliche Rollen des Staats bei der Umsetzung von E-Government und seinen einzelnen Komponenten denkbar. So kann er erstens als bloßer Rahmengeber auftreten, also rechtliche Vorgaben machen oder konkretere technische Richtlinien erlassen, beispielsweise durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Einen aktiveren Part nimmt der Staat ein, wenn er zusätzlich zum bloßen Rechts- und Ordnungsrahmen konkret (digitale) Identitäten als zentrale Teilkomponente der E-Government-Architektur anbietet, also beispielsweise den elektronischen Personalausweis, mit dem sich Bürger für Interaktionen mit der Verwaltung über das Internet identifizieren können. Die übrigen Komponenten der Architektur könnten in diesem Fall noch immer durch nicht staatliche Stakeholder entwickelt und bereitgestellt werden.

In seiner dritten, am weitesten ausgreifenden Rolle ist der Staat schließlich auch als Infrastrukturanbieter vorstellbar, und zwar konkret als Entwickler und Betreiber der gesamten E-Government-Infrastruktur.[50]

Außerdem möglich ist eine Public-private-Partnership (PPP) in unterschiedlichen Ausgestaltungen, mit staatsnahen Unternehmen oder anderen privatwirtschaftlichen Akteuren. So könnten die Aufgabenpakete der einzelnen Teilprojekte anteilig auf interne staatliche Ressourcen und externe private Dienstleister verteilt werden. Möglich wäre auch, die Erarbeitung und Durchführung einem oder mehreren privatwirtschaftlichen Akteuren zu überlassen, während Finanzierung und Kontrolle des Gesamtvorhabens beim Staat verbleiben.

Gerade bei digitalen Transformationsprozessen ist es eher Regel als Ausnahme, dass sich große Teile der internen Belegschaft – auch in Verwaltungen – nicht hinreichend mit den einzusetzenden und neuen Technologien auskennen. Dies kann zur Abwehrhaltung gegenüber den Umsetzungsmaßnahmen führen, wenn sich die betroffenen Personen überfordert und nicht ausreichend mitgenommen fühlen. Deshalb ist die sorgfältige und vor allem frühe Einbeziehung der Verwaltungsangestellten und Beamten in den Transformationsprozess einer der Schlüssel für eine erfolgreiche Umsetzung. Nicht zu unterschätzen ist zudem: Gerade intern gibt es meist ein umfassendes und wertvolles Wissen über die Details und Feinheiten der Verwaltungsprozesse, das für eine optimale Umsetzung genutzt werden sollte. Andere Fähigkeiten, die für den Digitalisierungsprozess notwendig sein können, fehlen wiederum gänzlich intern.

Es gibt also verschiedene Personen mit unterschiedlicher Herangehensweise und unterschiedlichem Wissensstand. Das gilt bei vielen privaten Digitalisierungsprojekten und wahrscheinlich noch stärker für die digitale Transformation staatlicher Verwaltungsstrukturen.

Diese Beobachtung verleitet leicht dazu, die Umsetzung der Digitalisierung der Verwaltung vollständig an ein oder mehrere private Unternehmen auszulagern. Eine solche Option mag sinnvoll sein, soweit es um abgeschlossene Projekte geht. Ein Projekt wie die schrittweise und sukzessive vollständige Digitalisierung etablierter Verwaltungsstrukturen erscheint hingegen zu komplex für ein Outsourcing an externe Experten. Ein solcher Schritt bietet sich am ehesten bei in sich abgeschlossenen Teilbereichen an.

Wie bereits dargelegt, wird bei digitalen Transformationen von Prozessen heute standardmäßig auf ein schrittweises und sich wiederholendes, also iteratives Vorgehen gesetzt. Es wird nicht möglich sein, ein vollständig konzipiertes Design und ein bis zum Ende gedachtes E-Government-System allein extern von einem oder mehreren privaten Unternehmen entwickeln und integrieren zu lassen. Gleiches gilt für die Frage nach der anschließend nötigen Wartung von außen. Allein der Aufwand, im Einzelfall Änderungs- bzw. Anpassungswünsche oder Fehler zu beschreiben und an die externe Firma zu übermitteln, ist mit beachtlichem zeitlichen Mehraufwand verbunden. Hinzu kommen steigende Kosten und das Risiko, dass sich auf diesem Kommunikationsweg vermehrt Fehler einschleichen können, die sich unter Umständen auf die Sicherheit des gesamten Systems auswirken.

50 Jens Fromm, Christian Welzel, Petra Hoepner, Jonas Pattberg, „Vertrauenswürdige digitale Identität: Baustein für öffentliche IT", Fraunhofer Fokus, Oktober 2013, *https://www.oeffentliche-it.de/documents/10181/14412/Vertrauensw%C3%BCrdige+digitale+Identit%C3%A4t+Baustein+f%C3%BCr+%C3%B6ffentliche+IT*, S. 8.

Ein privatwirtschaftliches Grundprinzip lautet, dass es stets möglich bleiben muss, eine nach außen vergebene Dienstleistung umfassend selbst zu beurteilen. Dies ist allerdings nur einer Person möglich, die selbst die dazu notwendigen Kompetenzen und Kenntnisse besitzt und nur deshalb zur Option des Outsourcings greift, weil zum Beispiel intern nicht ausreichend zeitliche Ressourcen zur Verfügung stehen.

Aufgrund dieser Erkenntnisse eignet sich Outsourcing höchstens in Teilbereichen für die Umsetzung von E-Government-Vorhaben. Welche Gestalt die digitale Transformation im Detail auch annehmen wird: Fortlaufende Änderungen und Anpassungen werden notwendig bleiben – sowohl am System selbst wie bei den Dienstleistungen. Dies folgt bereits aus der Grundentscheidung, einen nutzerzentrierten Ansatz bei der Implementierung der Architektur zu wählen. Bei einem solchen Vorgehen müssen die verschiedenen Software-Funktionalitäten laufend überprüft werden: auf ihre Wirksamkeit sowie daraufhin, ob sie von den Bürgern tatsächlich genutzt werden. Regelmäßige Befragungen und Nutzungsanalysen sind somit immanenter Bestandteil eines erfolgreichen nutzerzentrierten Ansatzes.

Statt einer bloßen Wartung und Instandhaltung werden also eine ständige Weiterentwicklung und fortlaufende Ausgestaltung notwendig sein. Befände sich das Know-how für diese Prozesse allein oder hauptsächlich in der Hand externer Akteure, liefe die Verwaltung Gefahr, laufend Kommunikationsschwierigkeiten ausgesetzt zu sein. Fehlendes internes Wissen müsste durch konstante Rückversicherung mit dem externen Dienstleister kompensiert werden. Ein solcher Übersetzungsaufwand ist weder effizient noch aus Kostensicht sinnvoll.

Wie könnte also eine primär interne Umsetzung aussehen? Und welche Voraussetzungen müssen für ihren Erfolg geschaffen werden? Ein bestimmter Teil des Bedarfs wird durch eine Umschulung oder Weiterbildung bestehender Mitarbeiter gedeckt werden können. Zudem müssen IT-Experten und Entwickler, die sich mit Programmiersprachen und der Weiterentwicklung von Systemen auskennen, als hausinterne Ressource eingestellt werden. Auch Experten für die Architektur der Infrastruktur sowie der Usability sollten den Mitarbeiterstab der Behörde ergänzen. Experten für IT-Sicherheit und Datenschutz, wie es sie zum Beispiel im Bundesamt für Sicherheit in der Informationstechnik sowie bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit gibt, müssen zusätzlich herangezogen werden.

Einen solchen Ansatz haben beispielsweise bereits jene Anwaltskanzleien verfolgt, die im Bereich „Legal Tech" tätig sind. Kanzleien, die sich nicht damit abfinden wollen, lediglich Anwender externer Tools zu sein, haben IT-Experten eingestellt, die „Legal Tech"-Anwendungen selbst entwickeln, anpassen und bei Bedarf erweitern.[51] Die Juristen allein könnten dies nicht selbst bewerkstelligen, und ein Outsourcing hätte nicht zu optimalen Ergebnissen geführt. Denn die Digitalisierung ist gerade eine interdisziplinäre Übung: Das gesammelte Wissen von fachlichen Praktikern und Entwicklern muss in ein derartiges Projekt fließen.

51 „Legal Tech"-Anwendungen sind beispielsweise Vertragsgeneratoren oder Tools, mit denen im Rahmen von Due Diligences in Rohdateien die relevanten Textbausteine erkannt und bewertet werden. Es wird erwartet, dass alle standardisierten Teile der Rechtsdienstleistung im Laufe der Zeit durch Technologie ersetzt werden können.

Die schnelle Entwicklung und die Komplexität der entwickelten und eingesetzten Systeme führen unweigerlich zu einem entsprechenden Bedarf an internem Personal, das hauptberuflich die digitale Verwaltung in ihrer Funktionalität und Sicherheit aufrechterhält und darüber hinaus die E-Government-Architektur um neue oder verbesserte Dienste erweitert. Daraus folgt: Der Staat muss auch für solche Entwickler, die zum Teil hohe Gehälter in der freien Wirtschaft erhalten, zum attraktiven Arbeitgeber werden. Denn wie gezeigt ist die Aufrüstung mit internem Know-how einer der Schlüsselaspekte für eine erfolgreiche digitale Transformation der Verwaltung.

Positioniert man die Verwaltung von Anfang an als Entwicklerin der Systeme statt nur als ihre Anwenderin, so können neu zu erschließende Bereiche und Anpassungen von Beginn an mitgedacht werden. Berater, die von außen kommen und Externe bleiben, kennen nur selten die Probleme und Herausforderungen interner Abläufe und sind darauf angewiesen, die notwendigen Informationen zu erfragen. Auch deshalb ist eine interne Abwicklung vorteilhaft.

Zwei weitere Aspekte sprechen für diese Vorgehensweise: Kontrolle und Unabhängigkeit. Ist der Staat bei der Umsetzung eines so elementaren Bereichs wie dem E-Government auf private Anbieter angewiesen, so begibt er sich in eine potenziell negative Abhängigkeit. So bieten viele große Tech-Unternehmen intransparente Dienstleistungen an, die möglicherweise nicht den strengen europäischen Datenschutzbestimmungen entsprechen. Aufgrund der fehlenden Transparenz können die Auftraggeber oft nicht verifizieren, ob die implementierte Technik den hiesigen normativen Anforderungen genügt. Mangels entsprechender faktischer Kontrollmöglichkeit muss er sich in diesen Fällen – trotz Sensibilität und Komplexität des Gesamtvorhabens – auf die Aussagen und Versicherungen des Anbieters verlassen.

Darüber hinaus sind E-Government-Projekte meist langfristig. In einem ständig fluktuierenden technischen und wirtschaftlichen Umfeld können die privaten Anbieter unerwartet in finanzielle Schwierigkeiten geraten. Aufgrund der Beschaffenheit und Komplexität des Auftrags ist es im Falle einer Insolvenz nicht möglich, ohne signifikante Friktionen einen anderen Anbieter zu wählen. Das birgt die Gefahr, dass die technische Lösung am Ende nicht optimal ist oder gar das Projekt neu gestartet werden muss.

Außerdem kann die Abhängigkeit von externen Dienstleistern zu Interessenkonflikten führen, wenn der Staat einerseits auf die privat angebotenen Dienste angewiesen ist, andererseits zugleich diese Unternehmen zu überprüfen und zu überwachen hat.

Letztendlich erhöht eine interne, eigene Umsetzung durch den Staat selbst sehr wahrscheinlich das Gefühl der Verantwortlichkeit und die Motivation innerhalb der eigenen Belegschaft. Wird ein Service selbst entwickelt, werden die Vor- und Nachteile sowie Herausforderungen jedes Schritts gemeinsam erarbeitet und diskutiert. Fehler werden so in der Regel schneller erkannt. Die E-Government-Architektur wird von der Verwaltung als eigenes Projekt angenommen, was einen weiteren Erfolgsfaktor für ein solch komplexes Großprojekt darstellt.

Schließlich sei erwähnt, dass die gängige Meinung, staatliche Strukturen könnten keine innovativen Ideen hervorbringen und umsetzen, schlicht falsch ist. So wurden in Deutschland zum Beispiel das Internet und die Mobilfunkkommunikation noch innerhalb des damaligen Bundespostministeriums umgesetzt.

Die Nutzung der E-Government-Architektur sollte den Bürgern kostenlos zur Verfügung gestellt werden. Sie sollte als Grundversorgungsprojekt für Bevölkerung und Unternehmen verstanden und definiert werden.

Zusammenfassend sprechen folgende Aspekte für eine verwaltungsinterne Umsetzung der digitalen Transformation zum E-Government:

1. Ohne internes Know-how kann die Umsetzung durch Externe kaum beurteilt werden.
2. Kosten- und zeitintensive Feedbackschleifen sind wahrscheinlich.
3. Eigene Belegschaft kann bei interner Umsetzung besser mitgenommen werden.
4. Die „Ownership" der Verwaltungsangestellten wird erhöht und das Verantwortungsgefühl und die Verantwortungsbereitschaft werden gesteigert.
5. Die Wartung von außerhalb ist fehleranfällig.
6. Mehr Kontrolle ist möglich.
7. Es entsteht keine Wettbewerbsverzerrung zugunsten großer Anbieter von IT-Dienstleistungen.
8. Der Staat bleibt unabhängig von privaten Unternehmen.
9. Staatliche Organisationen können gerade bei Großprojekten, die hohe finanzielle Aufwendungen erfordern, deutlich innovativer agieren.

5 TECHNISCHE UMSETZUNG

Der folgende Abschnitt erläutert und analysiert verschiedene Aspekte der technischen Umsetzung einer E-Government-Architektur und stellt ihre Kernfunktionen vor, wie sie in allen – im zweiten Kapitel beschriebenen – Nutzungsszenarien gebraucht werden. Dabei werden ebenfalls die oben dargelegten Aspekte der Nutzerfreundlichkeit und weiterer Qualitätsmerkmale berücksichtigt, die Voraussetzung für ein erfolgreiches Ausrollen von E-Government und einer tatsächlichen Nutzung durch Bürger und Unternehmen sind.

5.1. Kernfunktionspalette

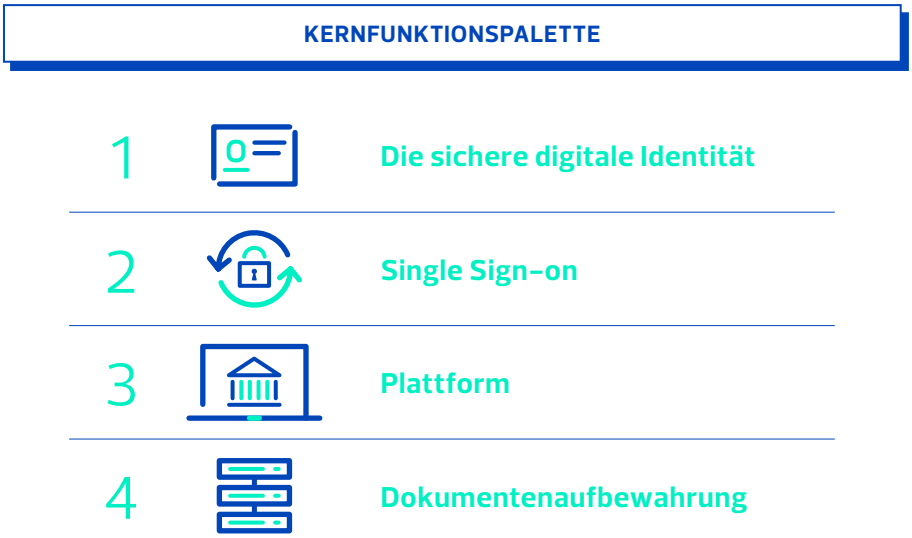
Im dritten Abschnitt wurde die grundsätzliche Notwendigkeit herausgearbeitet, die E-Government-Architektur schrittweise, modular und dem Prinzip der Nutzerfreundlichkeit folgend zu entwickeln.

Aufgrund der gebotenen iterativen technischen Entwicklung können nicht bereits vorab alle Umsetzungsmaßnahmen vorausgesehen werden. Es liegt in der Natur dieser Methode, dass sich die Maßnahmen und Module Schritt für Schritt im Laufe der Entwicklung ergeben. Dennoch gibt es natürlich Basisbausteine, ohne die eine E-Government-Architektur nicht auskommt. Deshalb sollte vor einer technischen Umsetzung die Palette der Kernfunktionen und der zentralen Module (engl. „Core Feature Set“) der zu implementierenden Systeme evaluiert werden, also jene Komponenten, die für jede Digitalisierung von Verwaltungsdienstleistungen elementar sind.

Betrachtet man die beschriebenen Szenarien im Jahr 2020, so benötigt der Bürger eine sichere digitale Identität, mit der er sich zum ersten Mal auf der Verwaltungsplattform einloggt – und die er immer wieder für die Authentifizierung nutzt.

Er benötigt außerdem einen sicheren Ort, an dem er seine wichtigen Dokumente aufbewahren und ablegen kann und von wo aus er entsprechende Zugriffsrechte differenziert nach Umfang und Zeitraum erteilen kann.

Zudem braucht er damit verbundene Zahlungsmethoden und weitere sogenannte Vertrauensdienste. All diese Komponenten müssen mit der Verwaltungsplattform verknüpft sein.

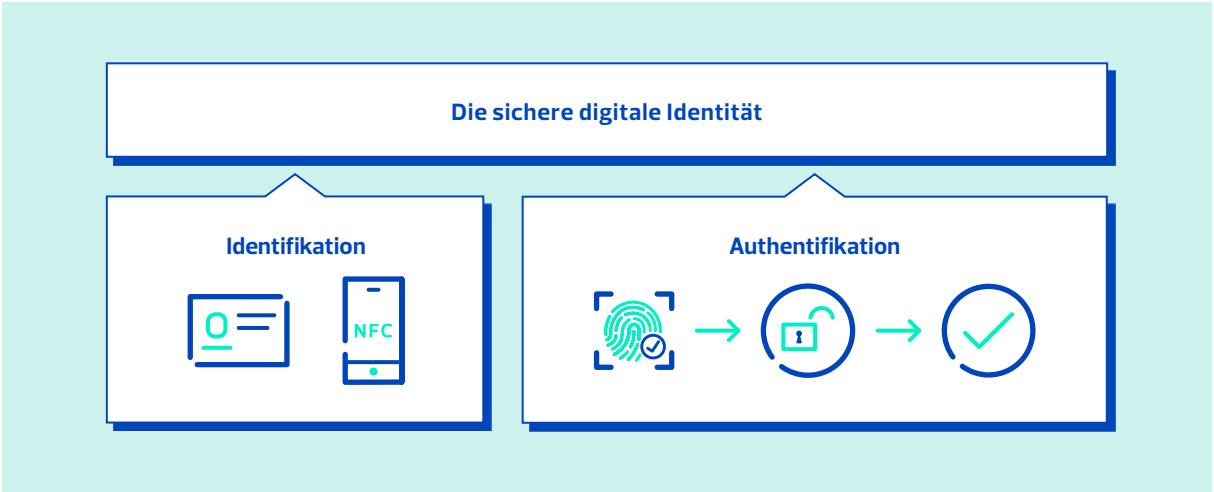


5.1.1 Sichere digitale Identitäten als Kernstück

Das im August 2017 verabschiedete Onlinezugangsverbesserungsgesetz (OZG) verpflichtet Bund und Länder einschließlich Gemeinden dazu, sämtliche Verwaltungsdienstleistungen bis Ende 2022 auch online anzubieten und über ein Portal zugänglich zu machen.[52] Als Ziel wurde die Umsetzung von über 500 Dienstleistungen bis zum Fristende avisiert. Derzeit findet die Evaluierung dieser Kerndienstleistungen statt.

52 Stefan Krempl, „IT-Großprojekt: Bürgerportal der Behörden soll bald testweise online gehen", heise online, 25. Juli 2017, *https://bit.ly/2v29HUZ*.

Herzstück einer jeden kostenlos zur Verfügung gestellten staatlichen Infrastruktur ist eine sichere digitale Identität. Mit dieser können Bürger und Unternehmen staatliche Verwaltungsdienste nutzen.



Für die Umsetzung sicherer digitaler Identitäten braucht es ein Identity- und ein Access-Management (Identifikation und Zugriff, kurz IAM), das eine zentrale Verwaltung von Identitäten und Zugriffsrechten auf unterschiedliche Systeme und Applikationen zulässt.

5.1.1.1 Identifikation

Mit Identifikation ist die Überprüfung gemeint, welche die Personalien (Identität, etwa Vor- und Zuname) einer natürlichen Person zuordnet.

Beantragt eine Person beispielsweise einen Personalausweis, so erfolgt die dazu notwendige Identifikation anhand der Kombination von bestimmten Urkunden (z. B. Geburtsurkunde), einem Foto der Person sowie dem persönlichen Erscheinen bei der zuständigen Behörde. Eine Identifikation im Internet ist derzeit bereits mittels des elektronischen Personalausweises und des elektronischen Aufenthaltstitels möglich. Für eine umfassende E-Government-Struktur ist diese Art der Identifikation jedoch möglicherweise nicht ausreichend. So ist nicht jede Person, die digitale Verwaltungsdienstleistungen in Deutschland nutzen möchte, notwendigerweise deutscher Staatsbürger oder verfügt über einen Aufenthaltstitel (z. B. EU-Bürger). Für sie – beispielsweise ausländische EU-Bürger, die in Deutschland arbeiten oder nur auf der Durchreise sind – muss eine Alternative angeboten werden.

Dies könnte die Identifikation per Smartphone sein, da die meisten ein solches ohnehin stets mit sich führen. Es erscheint daher sinnvoll, für die digitale Identität eine bereits weit verbreitete Hardware zu nutzen. Um sich per Smartphone zu identifizieren, bietet sich die Nutzung der NFC-Technologie (Near Field Communication) an. Mit ihr können Daten kontaktlos per Funktechnik über Strecken von wenigen Zentimetern übertragen werden. Anders als bei Bluetooth ist es nicht nötig, die beteiligten Geräte zunächst miteinander zu koppeln, und im Gegensatz zu Wireless LAN ist kein Einloggen erforderlich.

NFC wird bereits seit mehr als zehn Jahren im öffentlichen Nahverkehr in Deutschland genutzt. Auch die neuen Personalausweise verfügen über einen NFC-Chip, um eine sichere Authentifizierung zu ermöglichen. Inzwischen sind allerdings viele neue Dienste möglich, da immer mehr Hersteller von Smartphones solche Chips in ihren Geräten verbauen. Die Sicherheit der sensiblen personenbezogenen Daten wird durch die Ablage im „embedded Secure Element" (eSE) erhöht. Das eSE ist ein manipulationssicherer Chip, der in verschiedenen Größen und Ausführungen erhältlich ist, in jedes mobile Gerät integriert werden kann bzw. in vielen Geräten bereits integriert ist. Es stellt sicher, dass die Daten an einem sicheren Ort gespeichert werden und nur autorisierten Anwendungen und Personen Informationen zur Verfügung gestellt werden. Es ist wie eine persönliche ID für den Nutzer.

Die elektronische Identifizierung der Person mittels ihres Mobiltelefons wird somit möglich. Das gilt natürlich keineswegs nur für ausländische Personen, die sich in Deutschland aufhalten und keinen deutschen Personalausweis besitzen; auch deutsche Staatsbürger können sich alternativ für diese Variante entscheiden. Diese Auswahlmöglichkeit entspricht zugleich der bürgerzentrierten Ausgestaltung des E-Government-Vorhabens.

5.1.1.2 Authentifizierung, Autorisierung und der Sicherheitsaspekt

Der Authentifizierung genannte Vorgang dient dazu, dass der Nutzer gegenüber dem System belegt, dass er tatsächlich die Person ist, für die er sich ausgibt.[53]

Authentifizierungsmerkmale können zusätzlich zur Passwortabfrage auch Eigenschaften sein, die grundsätzlich untrennbar mit einer Person verbunden sind: die sogenannten biometrischen Merkmale. Gesichts- und Iriserkennung oder der Fingerabdruck sind solche physiologiebasierten Charakteristika. Diese unveränderlichen und einzigartigen Merkmale eignen sich besonders gut für eine schnelle Authentifizierung.

Jedoch muss bei der Diskussion über biometrische Daten auf die besonders hohen Sicherheitsrisiken hingewiesen werden: Die Begehrlichkeit Krimineller, an diese Daten zu kommen, ist besonders hoch. Wenn ein Fingerabdruck bereits kriminell eingesetzt wurde, ist das Merkmal sozusagen korrumpiert, denn anders als eine PIN kann man diesen Abdruck nicht ändern. Der Fingerabdruck ist nicht mehr nutzbar. In jüngerer Zeit ist darüber berichtet worden, dass beispielsweise die Terrormiliz IS gefälschte Fingerabdrücke für Finanztransaktionen nutzt.[54] Im sogenannten Dark Web sollen Hunderte Ausweise mit biometrischen Daten zu einem Marktwert von je rund 3.000 Dollar angeboten worden sein.

Aus diesem Grund kann die zentrale Relevanz von Sicherheitsstrukturen im Rahmen der Authentifizierung nicht genug betont werden. Dies gilt auch für die Sicherheit von Eingabegeräten. Die Ablage in einem eSE ist wichtig. Doch angesichts der Begehrlichkeit Krimineller, in den Besitz fremder biometrischer Daten zu kommen, braucht es eine erhöhte und lückenlose Kontrolle und eine stete Anpassung der Sicherheit. Sicherheitsvorfälle dieser Art bergen das Potenzial, die Akzeptanz und die Nutzung von E-Government zu gefährden und Schäden zu verursachen, die eine Rehabilitation des Systems erschweren.

Ist der Nutzer zweifelsfrei authentifiziert worden, geht es in einem nächsten Schritt darum, den Nutzer zu autorisieren. Dieser Vorgang legt fest, auf welche Systeme oder Ressourcen der Nutzer Zugriff erhält. Die Autorisierung basiert auf mehr oder weniger komplexen Regeln und Rollenkonzepten. Diese Regeln und Rollen können frei definiert oder von der Organisationsstruktur des Unternehmens und dem Arbeitsbereich des Nutzers abhängig sein.[55]

5.2 Single Sign-on

Eine weitere Kernkomponente der kostenlosen digitalen E-Government-Infrastruktur ist ein komfortabler, sicherer und zentraler Zugang, um auf die Verwaltungsdienste zugreifen zu können. Ein solches Single Sign-on ermöglicht es, sämtliche verfügbaren Dienste mit einem einzigen Account entweder am heimischen Computer oder per mobilem Endgerät zu nutzen. Dieser Zugangsweg ist zunächst dafür bestimmt, auf das Bürgerportal zuzugreifen und von dort aus mit der jeweils gewünschten Behörde zu interagieren. Ein solches Login sollte jedoch von Beginn an so konzipiert werden, dass sich auch privatwirtschaftliche

53 Hierfür wird sozusagen ein „Geheimnis" ausgetauscht. Es kommen mehrere Varianten in Betracht: von einer einfachen, aber nicht sehr sicheren Username/Passwort-Abfrage bis hin zu Mehrfaktorverfahren mit Security-Token oder der Nutzung verschiedener biometrischer Merkmale.

54 „Im Darknet blüht der Handel mit biometrischen Daten", Beitrag in der 12-Uhr-Ausgabe der Tagesschau vom 6. August 2018.

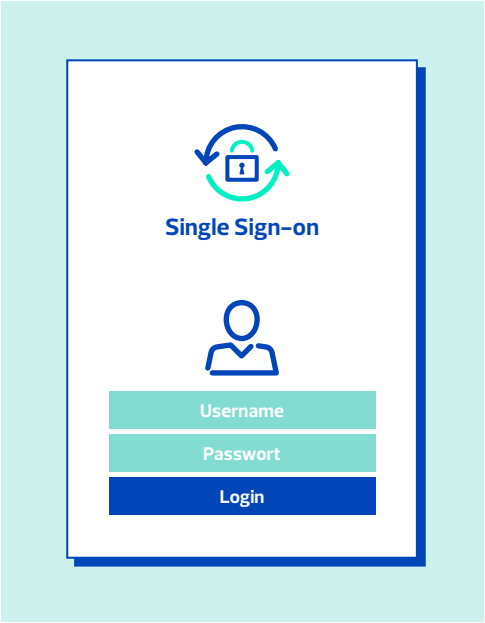
55 Peter Schmitz, „Was ist Authentifizierung?", Security Insider, 26. Juni 2017, *https://bit.ly/2K9ghOd*.

Anbieter von Dienstleistungen wie Banken oder Versicherungen auf eine Weise andocken können, die die Interaktion mit ihnen leicht über den zentralen Account ermöglicht. Für die letztgenannte Möglichkeit muss das System sicherheitstechnisch entsprechend ausgestaltet werden, um die nötige Datensicherheit garantieren zu können.

Der Erfolg von Facebooks Single Sign-on-Technologie (Facebook Connect)[56] zeigt, wie ein einfaches Login auf verschiedene Portale die Nutzung von Services im Internet erleichtern kann. Die Möglichkeit zur „Once only"-Eingabe der persönlichen Daten senkt die Schwelle zur erneuten und regelmäßigen Nutzung der Dienste deutlich.[57]

Aktuell lässt sich eine Situation mit paradoxen Zügen beobachten: Viele Bürger nutzen Facebook Connect, obwohl sie dem Anbieter Facebook in datenschutzrechtlicher Hinsicht zugleich misstrauen.[58] Schon aus diesem scheinbaren Widerspruch lässt sich herauslesen: Der Bedarf nach einem Single Sign-on-Verfahren, das zugleich bequem und sicher ist, ist beträchtlich.

Hier besteht die Chance, im Rahmen der Implementierung der digitalen Verwaltungsinfrastruktur eine relevante Lücke zu schließen. Gelänge es, den Zugang zum Bürgerportal als nutzerfreundliches, sicheres und offenes Login zu gestalten, könnte eine echte Alternative geschaffen werden, die der Bürger dann auch zentral und bequem für alle Logins nutzen kann, also auch um beispielsweise online einzukaufen.



Die vom Staat kostenlos zur Verfügung gestellte Version des Single Sign-on wird die Daten nicht mit dritten Akteuren der freien Wirtschaft teilen. Eine auf Gewinnabsicht zielende Analyse von Nutzungs-, Surf- oder Einkaufsverhalten ist somit ausgeschlossen. Daher können die Bürger sowie die Unternehmen bei der Nutzung Vertrauen aufbauen und somit freier agieren.

56 Vgl. Wikipedia, Facebook Platform, *https://bit.ly/2M2npOd.*

57 Elisa Schreiber, „How Facebook Connect changed the consumer internet", Techcrunch, 24. April 2016, *https://tcrn.ch/2M29FTA.*

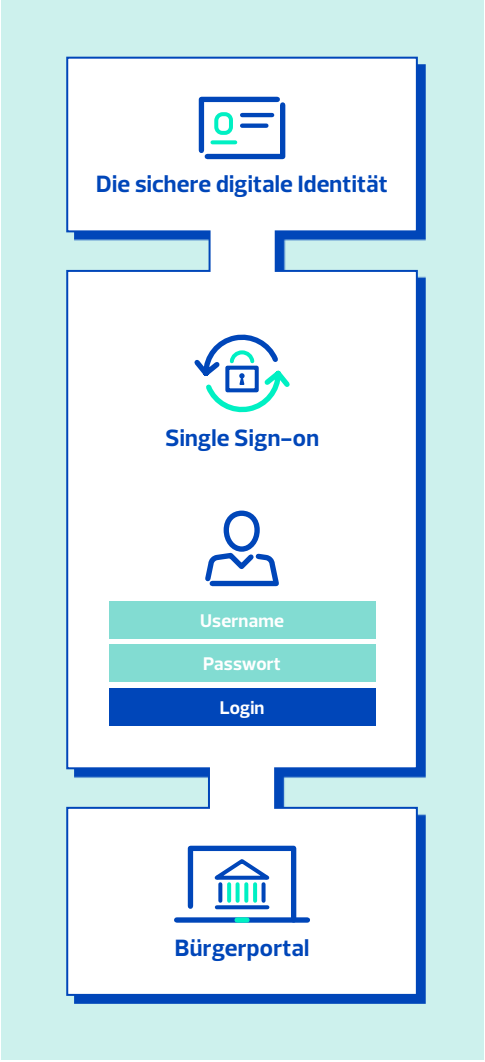
58 Beispielhaft unter vielen Studien mit ähnlicher Aussage aus dem Jahr 2017: Nahezu 80 Prozent der 1.600 befragten Leser von Quartz misstrauen Facebook. 58 Prozent der Teilnehmer der Umfrage stammen aus den USA, wo der Umgang mit sozialen Plattformen sogar als unkritischer gilt (*https://qz.com/1085588/survey-facebook-is-the-bigtech-company-that-peopletrust-least/*).

5.3 Plattform

Im Zielbild der Verwaltungsplattform kommen alle Verwaltungsdienstleistungen, sämtliche Informationen und Dokumente sowie die Möglichkeit, Zahlungen zu veranlassen, zusammen. Dort sind sie zentral verfügbar und abrufbar.

Neben dem leichten und intuitiven Zugang sind die Architektur und die Qualität der Plattform selbst entscheidend. Denn eine vertrauenswürdige Serviceplattform fungiert als Kommunikationsschnittstelle zwischen den Akteuren Bürger/Unternehmen auf der einen und der Verwaltung auf der anderen Seite.

59 Koalitionsvertrag 2018, S. 45.



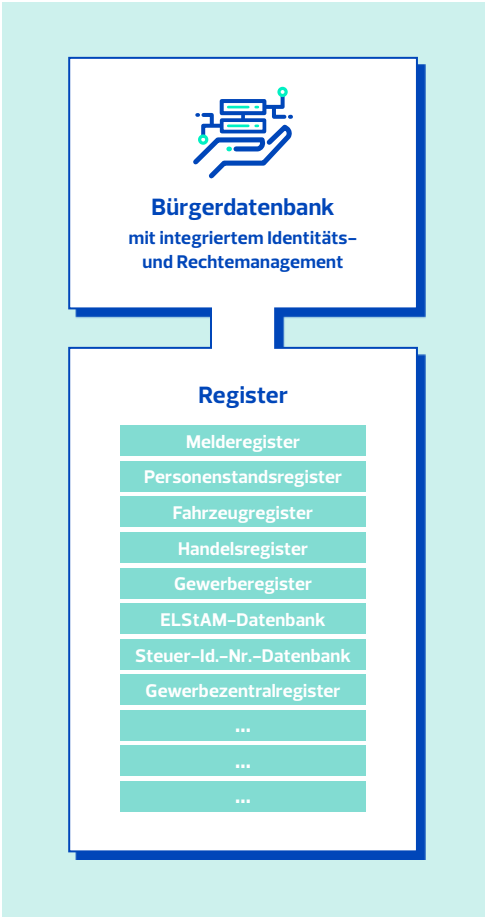
Die E-Government-Plattform sollte die folgenden Vertrauensdienste als notwendige Komponenten beinhalten:

- Einen sicheren Speicher für private Daten und Dokumente
- Die Möglichkeit zur Abfrage und automatischen Übermittlung von Dokumenten und anderen Daten in passende Prozesse
- Die Authentizitätsprüfung der Daten und Dokumente (d. h. digitale Signatur)

Auf diese Weise kann die Plattform die digitalen Verwaltungsprozesse ermöglichen und vereinfachen.

Der Koalitionsvertrag 2018 sieht die baldige Einrichtung einer solchen Plattform vor. Mit dem Bürgerportal genannten Service soll den Bürgern ein einfacher und sicherer Zugang zu vielen Verwaltungsdienstleistungen zur Verfügung gestellt werden.[59]

5.4 Dokumentenablage / Dokumentenverwaltung



Ob Geburtsurkunden oder Schulzeugnisse, Versicherungsverträge oder Krankenakten, Steuerunterlagen oder Zeugnisse: Die Szenarien im zweiten Kapitel zeigen auf, wie der zentrale Datenzugriff und die Möglichkeit zu wiederholten Uploads nach dem Heraussuchen von Dokumenten einen erheblichen Mehrwert für E-Government-Angebote bieten.

In einem nutzerzentrierten, sicheren System liegen alle wichtigen Dokumente eines Menschen nach Bedarf für ihn bereit – unabhängig davon, bei welcher Organisation sie gespeichert sind. Mittels einer digitalen Vergabe von Berechtigungen kann der Bürger jederzeit Dritten Einblick gewähren und genauso diese Berechtigung wieder entziehen.

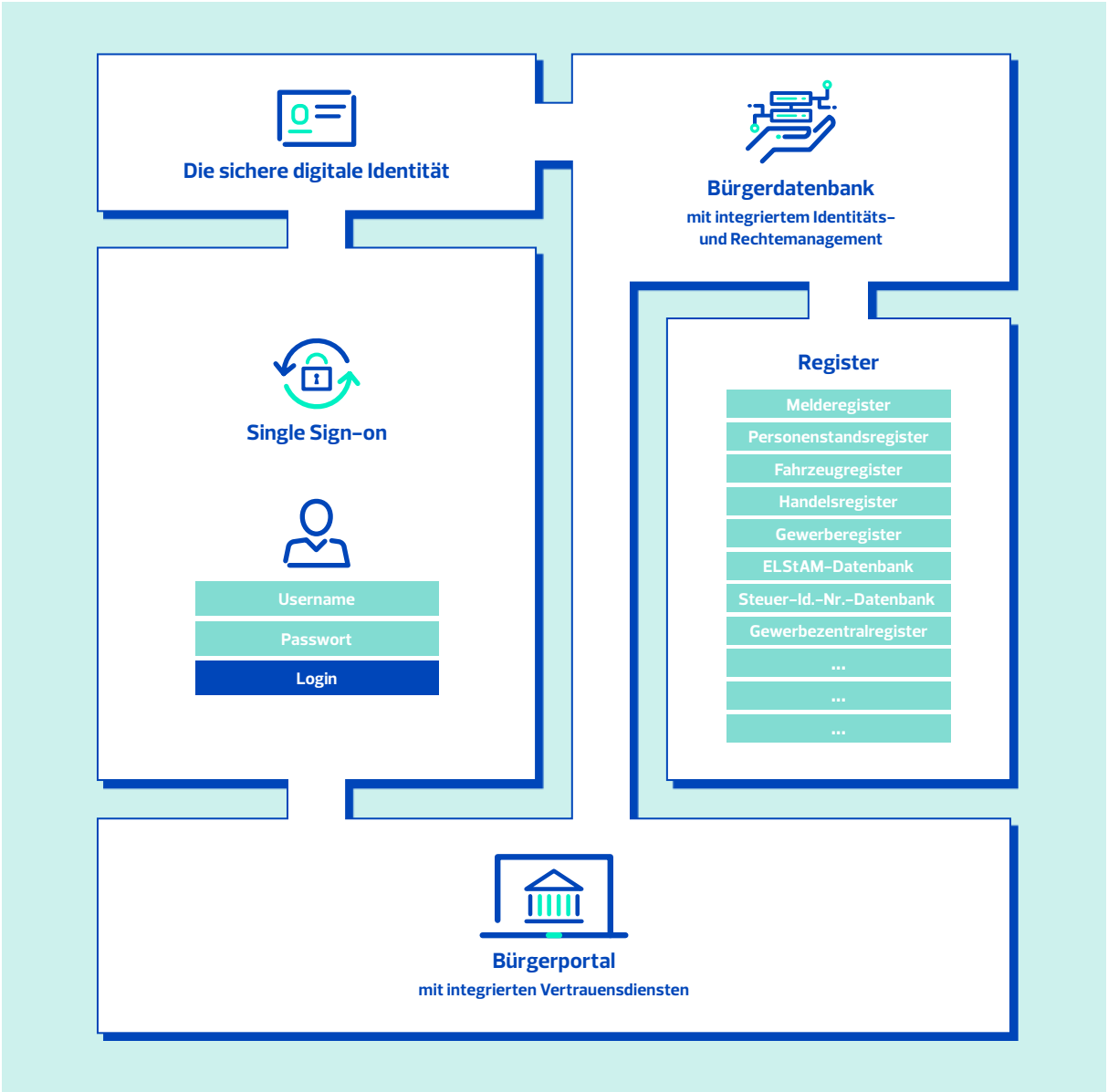
Bei einem nutzerzentrierten Ansatz erhalten Bürger und Unternehmen die volle Autorität und das Selbstbestimmungsrecht, jederzeit souverän über ihre Daten und deren Weitergabe zu entscheiden.

Um dieses Recht faktisch zu gewährleisten und umzusetzen, bedarf es eines neuen Ansatzes: Die Steuerung des Identitäts- und Rechtemanagements wird in die Hände der Bürger sowie Unternehmen gelegt. Sie behalten stets die Kontrolle über ihre Daten und erteilen und entziehen selbst die Zugriffsrechte. Auch haben nur sie die volle Autorität, entsprechende Berechtigungen bei Bedarf an andere Personen oder Entitäten zu delegieren. Die Verwaltung der Dokumente erfolgt genauso wie die digitale Vergabe von Berechtigungen durch den Nutzer selbst. Diese umfasst Dokumente, die in seinem Herrschaftsbereich auf einem internen Server oder einem externen Server (Cloud) liegen, und zudem den Zugriff auf unterschiedliche staatliche Register. Dieses Konzept funktioniert auch dann, wenn die personenbezogenen Daten der Bürger – zumindest in den kommenden Jahren – realistischerweise parallel in unterschiedlichen Registern abgelegt sind. Die Registerlandschaft in Deutschland ist stark zersplittert. Kammern und Verbände führen zum Beispiel Register über ihre Mitglieder (Zulassungen, Befähigungen etc.); die Krankenkassen und Sozialversicherungsträger verarbeiten Gesundheits- und Sozialdaten; Behörden wiederum führen Verwaltungsdaten im Rahmen ihrer Aufgaben (z. B. Meldebescheinigung, Führerschein). Eine Modernisierung des Ist-Zustands ist geplant. Dies wird jedoch aufgrund der Verflechtungen und unterschiedlichen Interessen ein langwieriger Prozess. Die oben aufgezeigte Lösung kann mit dem Status quo umgehen und Schritt für Schritt auf die Modernisierung mit Anpassungen reagieren, ohne auf ihren Abschluss warten zu müssen. Von möglichen Inkonsistenzen zwischen Registern abgesehen ist eine solche doppelte Ablage grundsätzlich unschädlich und erfordert deshalb keine Vorabentscheidung über die Zusammenlegung und Modernisierung von Registern.

Dass der Bürger zentral auf seine relevanten Daten zugreifen kann, ist ein längst überfälliger Schritt in Richtung Datensouveränität. Dies entspricht den Erwartungen der Nutzer und den

Anforderungen der Datenschutz-Grundverordnung (DSGVO) im Sinne des „Privacy by Design"-Ansatzes: vollständige Transparenz für den Nutzer und keine Einsichtsmöglichkeit für alle anderen (engl. „Zero Knowledge"), jedenfalls solange diese keine entsprechende Berechtigung durch den Nutzer erhalten oder aufgrund einer sonstigen rechtlichen Grundlage Zugang haben. In besonderem Maße gilt dies für den sensiblen Bereich der Datenablage.

Eine bürgerfreundliche Sicherheitsarchitektur



5.5 Qualitätsmerkmale

Eine solche Integration von Datenschutz und -sicherheit in die Entwicklung der künftigen E-Government-Architektur wäre eine echte Innovation. Eine derartige Architektur bereitet den Weg für eine echte und umfassende Einbettung dieser Systeme in den Alltag der Bürger. Zudem nimmt ein solcher Ansatz das immer noch junge, zunehmend wichtiger werdende Grundrecht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme ernst und bringt es im Verhältnis zwischen Bürger und Staat zur Geltung.[60]

Die bürgerzentrierte Herangehensweise gewährleistet dem Bürger stets die Datensouveränität bei der Nutzung des Portals und das Management der Zugriffsrechte auf Urkunden und Dokumente. Nicht nur die Möglichkeit, sondern auch die Verantwortung wird auf den Bürger übertragen.[61]

Bei der Entwicklung dieser Grundbausteine bzw. notwendigen Komponenten in der Architektur eines E-Government-Projekts ist das Dreieck aus Sicherheit, Datenschutz bzw. -souveränität und Nutzerfreundlichkeit in jedem einzelnen Schritt – also by Design – mit zu bedenken und zu implementieren.

Diese notwendigen Qualitätsmerkmale sind Voraussetzung dafür, dass das für den Erfolg der E-Government-Architektur erforderliche Vertrauen auf Seiten der Bürger aufgebaut wird und es tatsächlich zur Nutzung der digitalen Angebote kommt.

Nicht erst seit Inkrafttreten der DSGVO steht das Selbstbestimmungsrecht der Nutzer – also ihre tatsächliche Möglichkeit, über Verarbeitung und Weitergabe ihrer personenbezogenen Daten selbst zu entscheiden – politisch im Vordergrund. Eine Umsetzung des Vorhabens der digitalen Transformation der Verwaltung ohne Beachtung dieses Prinzips der Datensouveränität als Teil einer umfassenden digitalen Souveränität ist praktisch nicht vorstellbar.[62]

Die drei oben genannten Aspekte erst später zu einer bereits weitgehend fertiggestellten Architektur hinzuzufügen wäre – falls überhaupt technisch möglich – mit unverhältnismäßig

60 Das Grundrecht der Integrität der IT-Systeme wurde in den Leitsätzen des Urteils des Bundesverfassungsgerichts vom 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07, BVerfGE120, 274 – neu formuliert.

61 Zu den damit zusammenhängenden Herausforderungen siehe Punkt 6.3.

62 Vgl. zum Begriff Deutscher Ethikrat, „Big Data und Gesundheit – Datensouveränität als informationelle Freiheitsgestaltung", Stellungnahme, 30. November 2017, *https://bit.ly/2K6vAax*, S. 251 ff.

hohem Kosten- und Zeitaufwand verbunden. Daher erscheint die Vorabberücksichtigung und -einflechtung sinnvoll.

Die wichtigsten Funktionen und Merkmale einer digitalen Verwaltungsinfrastruktur seien nachfolgend noch einmal knapp zusammengefasst:

1. Authentifizierung und Autorisierung von Benutzern
2. Zentrale Zugriffsplattform mit integrierten Vertrauensdiensten
3. Single Sign-on für den Zugriff auf unterschiedliche Systeme und Ressourcen mit einer einzigen Identität
4. Zentralisierte Verwaltung von Identitäten und Zugriffsberechtigungen
5. Nutzerzentrierung, d. h. souveräne Verteilung und Kontrolle von Zugriffsrechten auf Dokumente durch Bürger und Unternehmen

5.6 Weitere technische Aspekte der Umsetzung

5.6.1 Skalierbarkeit und Weiterentwicklung

Die technische Umgebung bei der digitalen Transformation der Verwaltung ist nicht statisch. Technologien ändern sich stetig. Neue interne oder externe Anforderungen bringen es mit sich, dass Systeme angepasst und weiterentwickelt werden müssen. Daher kann die Digitalisierung niemals als eine einmalige Umstellung auf eine bestimmte, zuvor ausgewählte „Software X" gedacht werden. Im Gegenteil: Wahrscheinlich müssen notwendige Anpassungsleistungen künftig in immer kürzeren Abständen vollzogen werden. Notwendig ist, wie bereits als konzeptuelle Grundprämisse begründet, ein iteratives Vorgehen in Verbindung mit einer Offenheit gegenüber dem Prinzip „Trial and Error" – zwar keineswegs bei der Sicherheit der Produkte, aber bei der Entwicklung neuer Komponenten – und der regelmäßigen Konfrontation mit Betaversionen, die zunächst weiterer Testläufe bedürfen.

Zu diesem Zweck ist von staatlicher Seite eine an Qualitätssicherung und -kontrolle („Quality Assurance", kurz QA) angelehnte Abteilung einzurichten, die Hard- und Software der E-Government-Architektur laufend wartet, stets mit Updates auf dem neuesten Stand hält und zudem durch stetige Testdurchgänge die Funktionalität und Sicherheit der Systeme gewährleistet.

Für einen hohen Sicherheitsstandard muss laufend aktiv nach möglichen Sicherheitslücken Ausschau gehalten werden. Wird eine solche entdeckt, ist sie unverzüglich zu schließen. Zudem sollte ein differenziertes Vorgehen im Einklang mit den Vertrauensstufen

gewählt werden, wie es die EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO) vorsieht[63] – also „Security by Design", angepasst an die Sicherheitsstufen bestimmter sensibler Bereiche. Eine solch kleinteilige Vorgehensweise erfordert eine ausreichende Zahl interner Fachkräfte, die eben nicht lediglich als ein bloßer Wartungsdienst agieren, sondern Systeme testen und bei Bedarf selbst weiterentwickeln können.

63 Siehe zur Verordnung unten, Kap. 6.1.

Grundsätzlich sollte möglichst lange technologieneutral geplant werden, und zwar so, dass es immer möglich bleibt, sich auf ständig ändernde digitale Technologien einzustellen. Die Entwicklung der Architektur muss diese Anpassungsfähigkeit integrieren und eine skalierbare und flexible Struktur bieten, die stets offen genug für Weiterentwicklungen bleibt: „Scalability by Design".

5.6.2 Integration von Blockchain-Technologien

Eine noch relativ junge und insbesondere für E-Government interessante Technologie ist die sogenannte Blockchain. Dabei handelt es sich vereinfacht gesagt um ein elektronisches Register für digitale Datensätze, Ereignisse oder Transaktionen, die durch die Teilnehmer eines verteilten Rechnernetzwerks verwaltet werden.[64] Auch die Bundesregierung hat bereits ihr Interesse an der Nutzung der Technologie geäußert. Laut Koalitionsvertrag vom Februar 2018 wird die Bundesregierung innovative Technologien wie „Distributed Ledger" (Blockchain) erproben.[65]

64 Vincent Schlatt et al., „Blockchain: Grundlagen, Anwendungen und Potenziale", White Paper, Fraunhofer-Institut für Angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik, 2016, *https://bit.ly/2M23WwY*, S. 8.

65 Koalitionsvertrag 2018, S. 45.

Bisherige Technologien lösen das Nutzerbedürfnis nach Kontrolle über ihre Daten nur unzureichend ein. Mithilfe der Blockchain hingegen kann schon in der Basistechnologie die oben beschriebene Datensouveränität durch ein Rechtemanagement-System verankert werden. So können Berechtigungsketten gestaltet werden, die auf der Blockchain liegen und allein dem jeweiligen Nutzer die Kontrolle über die digitalen Berechtigungen wie den Zugriff auf bestimmte Dokumente geben. Für jedes Recht – etwa auf ein über das Bürgerportal abgelegtes Dokument zugreifen zu dürfen – kann der Bürger als einziger verantwortlicher Rechteeigentümer bestimmt werden. Nur er kann die Berechtigung an andere – zweckgebunden – delegieren und anschließend wieder entziehen. Dabei ist ein variabler Ansatz denkbar: So können die Berechtigungen unterschiedlich gestaffelt werden; manche könnten beispielsweise gar nicht delegiert, andere nur begrenzt weitergegeben werden.

In diesem Modell sieht jeder Akteur stets nur das, wofür er auch die entsprechende Berechtigung besitzt. In einem E-Government-Konzept, das – wie hier vertreten – von Grund auf „Privacy by Design" mitdenkt und integriert, müsste die Berechtigungsverwaltung so ausgestaltet werden, dass sie den Bürgern die alleinige Verfügungsgewalt überlässt. Die Bürger selbst müssen als Administratoren ihres Datenbestands die Zugriffsrechte verwalten.

Die Blockchain-Technologie kann für eine solche sichere und nachvollziehbare Verwaltung von digitalen Identitäten und Berechtigungen geeignet sein und verdient eine nähere

Betrachtung.[66] Allerdings sollten einige ihrer Eigenschaften modifiziert werden, bevor sie im Rahmen der E-Government-Architektur eingesetzt werden kann.

So erfolgt die Verkettung der einzelnen Datenblöcke grundsätzlich nur in eine Richtung, was zu Redundanzen führt und die Rechenintensität erhöht. Dies ließe sich durch eine bidirektionale Verkettung auflösen. In Verbindung mit einer Komprimierung wären die Datenintensität und der Bedarf an sehr großen Speicherkapazitäten geringer.

Zudem ist wiederholt angemerkt worden, die Blockchain-Technologie sei problematisch im Hinblick auf die Vorgaben der Datenschutz-Grundverordnung. So sei angesichts ihrer fundamentalen Funktionsweise nicht klar, wie datenschutzrechtliche Ansprüche wie das Recht auf Löschung oder das Recht auf Berichtigung gespeicherter Sätze personenbezogener Daten in der Blockchain realisiert werden könnten.[67] Dies kann allerdings durch eine nachträgliche Löschung oder Änderung von Hash-Werten ermöglicht werden, so dass Konformität erreicht werden kann. Zudem können Blöcke mit besonders sicherheitskritischen Informationen oder sensiblen Daten in übergreifenden Funktionen quasi versteckt werden.

Hinsichtlich der Flexibilität und Performanz bedarf es weiterer Forschung auf dem Gebiet der Blockchain. Hinzu kommt das Problem des hohen Energiebedarfs, das ebenfalls bei den Überlegungen zum Einsatz der Technologie eine maßgebliche Rolle spielt. Energieintensive Konsensus- und Mining-Verfahren, wie sie bislang meist zum Einsatz kommen, können ersetzt werden, wenn keine replizierte Datenbank im klassischen Verständnis der Blockchain verwendet wird. Solche Optionen wären im Sinne einer nachhaltigen Blockchain-Lösung.

Eine solche Entscheidung zur Evaluierung erscheint gerade im Hinblick auf die Blockchain-Technologie sinnvoll, da ihre Dezentralität die föderale Struktur Deutschlands sehr gut widerspiegelt. Vor allem aber aus Sicherheitserwägungen stellt die Blockchain eine sehr interessante Entwicklung dar, die bei der Konzeption der E-Government-Architektur berücksichtigt werden sollte.

5.6.3 Integration von künstlicher Intelligenz

Ein weiterer aktueller Trend ist die künstliche Intelligenz. Das Thema ist breit gefächert – und selbst die Frage, was künstliche Intelligenz eigentlich ist und wie sie definiert werden sollte, ist sehr umstritten. Derzeit gibt es unübersichtlich viele Spielarten und Verständnisse: angefangen beim Einsatz von Algorithmen zur Erkennung und Analyse von Mustern über automatische algorithmische Entscheidungsfindung bis zu vollständiger Emulation menschlicher Intelligenz und menschlichen Verhaltens.

Bei der Umsetzung des hier beschriebenen E-Government-Projekts ist ein Einsatz künstlicher Intelligenz an verschiedenen Punkten denkbar. So wird eine automatische Bilderkennung bei der Authentifizierung und Autorisierung bereits eingesetzt. Zudem

66 Berechtigungen können in verschiedenen Ausprägungen erfolgen, so zum Beispiel in Form biometrischer Daten oder durch den Einsatz von Zertifikaten.

67 Helen Bielawa, „DSGVO: Motor oder Bremse für die Blockchain-Technologie?", *t3n.de*, 26. Mai 2018, *https://bit.ly/2K8laad*.

eignet sich künstliche Intelligenz im weitesten Sinne für Standardaufgaben, die sich immer wiederholen. Jene Aspekte der Verwaltungstätigkeit, die auf solche repetitiven Aufgaben reduzierbar sind, werden sicher in besonderem Maße von der fortschreitenden Automatisierung betroffen sein und sind strukturell offen gegenüber künstlicher Intelligenz.

Allerdings gilt: Bei jedem Schritt hin zu mehr Automatisierung und ganz allgemein beim Einsatz von Anwendungen, die auf künstlicher Intelligenz beruhen, sind stets alle Umstände in die Nützlichkeitsanalyse mit einzubeziehen. Die Sinnhaftigkeit des Einsatzes ist ergebnisoffen und kritisch zu evaluieren. Ein weiterer Aspekt ist die teilweise fehlende Nachvollziehbarkeit algorithmischer Entscheidungsfindung, das sogenannte Black-Box-Problem. Dazu wird bereits unter dem Begriff „explainable AI" geforscht. Diese Ergebnisse bleiben vor einer Implementierung abzuwarten, da besonders im Verhältnis zwischen Staat und Bürger die Nachvollziehbarkeit eine besonders große Rolle spielt. Bloße Machbarkeit sollte gerade nicht der ausschlaggebende Punkt sein. Vor allem sollte die Verwendung künstlicher Intelligenzen niemals im Widerspruch zu den oben herausgearbeiteten Prinzipien stehen: Der Einsatz muss die Bürgerzentriertheit der Gesamtarchitektur bewahren und sollte mit den Grundsätzen der Nutzerfreundlichkeit im Einklang stehen. Aus der Binnenperspektive der Verwaltung wäre es zugleich wünschenswert, wenn der Einsatz von KI-Technologien keinen größeren Personalabbau zur Konsequenz hätte. Künstliche Intelligenz hat dann das Potenzial, zum Erfolgsmodell zu werden, wenn sie als Erweiterung menschlicher Fähigkeiten begriffen wird, nicht als ihr Ersatz.

5.6.4 Offene und erweiterbare Systeme

Wie bereits angedeutet, sollten die technischen Systeme, die für die digitale Verwaltung aufgesetzt werden, flexibel und erweiterbar sein. Dafür müssen sie offen sein: Diese Offenheit ist zum einen als Skalierbarkeit und Flexibilität zu verstehen. Zum anderen sollte der Code, der dem System zugrunde liegt, öffentlich einsehbar sein – selbstverständlich nur insoweit, als dies nicht die Sicherheit der Architektur gefährdet. Und drittens gilt die Offenheit für neue innovative Ansätze sowohl hinsichtlich Sicherheit wie Nutzerfreundlichkeit.

Ein auf diese Weise offener Ansatz hätte den Vorteil, dass zum Beispiel interessierte Akteure wie Forschungsinstitute an Hochschulen die Systeme in eigener Initiative ausbauen und sie anschließend der Verwaltung wiederum zur Verfügung stellen könnten. Absolventen dieser Hochschulen, die bereits im Rahmen ihres Studiums mit den digitalen Verwaltungssystemen vertraut gemacht wurden, könnten unkompliziert zu späteren Verwaltungsangestellten ausgebildet werden und dann intern an der Fortentwicklung der E-Government-Architektur weiterarbeiten. Auf diese Weise könnten sich die Bereiche gegenseitig befruchten. Es entstünde für die kommenden Jahre ein Personalkreislauf, der weitgehend unabhängig von der Privatwirtschaft wäre. Wie auch immer die Zusammenarbeit mit Hochschulen und Forschungsinstituten genau gestaltet sein wird: Es muss einen regen Austausch geben, um die Anforderungen der Bürger sicher, datenschutzkonform und nutzerfreundlich umsetzen zu können.

6 VORAUSSETZUNGEN UND PARAMETER DES AUFBAUS VON E-GOVERNMENT-STRUKTUREN IN DEUTSCHLAND

In den bisherigen Abschnitten wurde untersucht, welche organisatorischen und technischen Aspekte beim Aufbau von E-Government als Grundversorgungsprojekt in Deutschland zu beachten sind, einschließlich sicherer digitaler Identitäten als sein notwendiger Kern. Selbstverständlich wird ein solch umfassendes und komplexes Vorhaben nicht nur durch diese Erwägungen bestimmt. Im Folgenden werden daher, als Handreichung für Entscheider, kurz die wichtigsten nicht technischen Voraussetzungen und Parameter für die Umsetzung der oben konzipierten E-Government-Architektur dargestellt. Dabei geht es in erster Linie um die rechtlichen und politischen Rahmenbedingungen, zudem um gesellschaftliche und ethische Fragen.

6.1 Rechtliche Rahmenbedingungen und Herausforderungen

6.1.1 Europäische Rahmensetzung

Wie bereits mehrfach beschrieben, bewegen sich die Bemühungen, eine E-Government-Architektur in der Bundesrepublik aufzubauen, innerhalb eines größeren europäischen Rahmens. So verkündete die Europäische Kommission im April 2016 ihren „EU eGovernment Action Plan 2016-2020", der die digitale Transformation der Verwaltungen der EU-Mitgliedsstaaten als zentrales Element für den Erfolg des Binnenmarkts im 21. Jahrhundert identifiziert.[68] Der Plan macht keine direkten europarechtlichen Vorgaben. Er soll jedoch den zuständigen öffentlichen Akteuren in den Mitgliedsstaaten gewisse Leitlinien vorgeben, um bis zum Jahr 2020 den Bürgern sowie Unternehmen in der gesamten EU eine grenzenlose, personalisierte, nutzerfreundliche und vollständig digitale öffentliche Dienstleistungsinfrastruktur bereitzustellen.[69] Eines der wesentlichen Elemente des Action Plans ist der „eGovernment Benchmark Report", mit dem die EU-Kommission die Fortschritte in den europäischen Staaten beim E-Government an vier wesentlichen Indikatoren (Nutzerzentriertheit, Transparenz, grenzüberschreitende Mobilität, Schlüsseltechnologien) evaluiert.[70]

Während ihrer jüngsten EU-Ratspräsidentschaft in der zweiten Jahreshälfte 2017 war die estnische Regierung bemüht, ihrer allgemein anerkannten Vorreiterrolle bei der Umsetzung von E-Government gerecht zu werden. Mit der „Tallinn Declaration on eGovernment" wurde auf ihre Initiative im Oktober 2017 von Ministern aus 32 EU- und EFTA-Staaten, die für die Digitalpolitik in ihren Ländern zuständig sind, eine Erklärung mit weiteren Zielsetzungen vereinbart, die auf dem „EU eGovernment Action Plan 2016-2020" aufbaut.[71] Das Dokument enthält insbesondere sogenannte „Policy action lines", in denen die oben genannten Leitprinzipien, die im Action Plan niedergelegt sind, weiter ausformuliert wurden.

68 European Commission, „Communication: EU eGovernment Action Plan 2016-2020 – Accelerating the digital transformation of government", 19. April 2016, *https://bit.ly/1pdCgsD*.

69 Ebd., S. 2.

70 Siehe den Report für 2017 unter *https://bit.ly/2BmNS3X*.

71 Tallinn Declaration on eGovernment at the ministerial meeting during Estonian Presidency of the Council of the EU, 6. Oktober 2017, *https://bit.ly/2xYu9WX*.

So geht es im Abschnitt „Vertrauenswürdigkeit und Sicherheit" darum, auf nationalstaatlicher Ebene als Grundgerüst der E-Government-Infrastruktur sichere digitale Identitäten zu etablieren. Um hier Vertrauen herzustellen, wird auf den eIDAS-Rechtsrahmen für qualifizierte elektronische Vertrauensdienste verwiesen, der unter Punkt 6.1.4 näher erläutert wird. Unter „Offenheit und Transparenz" wird das Grundprinzip des bürgerzentrierten Identitätsmanagements noch einmal hervorgehoben. Bürger sowie Unternehmen sollen ihre persönlichen Daten, die digital bei der Verwaltung gespeichert sind, selbst online managen können – also mit ihrem eigenen Endgerät auf sie zugreifen, sie überprüfen, ihre Verwendung nachvollziehen, bei Bedarf berichtigen lassen und die Verarbeitung autorisieren. unter Punkt „Standardmäßige Interoperabilität" wird den beteiligten Staaten empfohlen, auf offene Standards und die Verwendung von Open-Source-Software zu setzen.

Im Annex der Tallinn Declaration schließlich befinden sich die „Prinzipien der Nutzerzentriertheit für das Design und die Erfüllung digitaler öffentlicher Dienstleistungen", zu deren Umsetzung sich die EU- und EFTA-Staaten bekennen. Diese Prinzipien sind:

- Digitale Interaktion
- Erreichbarkeit (Barrierefreiheit), Sicherheit, Verfügbarkeit und Nutzerfreundlichkeit
- Reduktion der Belastung der Verwaltung
- Digitale Erfüllung öffentlicher Dienstleistungen
- Bürgerengagement
- Anreize, die digitalen Dienste zu nutzen
- Schutz der personenbezogenen Daten und der Privatsphäre
- Mechanismen für Beschwerdeverfahren und Entschädigung

Sowohl der Action Plan der EU-Kommission als auch die Tallinn Declaration mit ihren „Prinzipien der Nutzerzentriertheit" bestätigen die zentrale Bedeutung des Fokus auf die Perspektive der Bürger und die Sicherstellung echter Datensouveränität beim Nutzen von E-Government-Dienstleistungen. Der Infrastruktur muss zudem stets die sichere digitale Identität der Nutzer zugrunde liegen. Auch wenn es sich bei diesen Dokumenten nicht um im eigentlichen Sinne strenge europarechtliche Vorgaben handelt, hat sich die digitale Transformation der Verwaltung in Deutschland an diesen Leitlinien zu orientieren. Erfolgt die Umsetzung so, wie in den Kapiteln 4 und 5 dieser Studie empfohlen, dann ist diesen Voraussetzungen Genüge getan.

6.1.2 Staatsorganisationsrechtliche Fragen

Gemäß dem „eGovernment Benchmark Report 2016" der EU-Kommission hinkt Deutschland bei der Umsetzung von E-Government-Maßnahmen gegenüber anderen europäischen Staaten deutlich hinterher. Als einer der wesentlichen Gründe wurde die föderale Struktur der Bundesrepublik identifiziert. Diese verhindert, dass Umsetzungsmaß-

nahmen effektiv von einer einzigen zentralen öffentlichen Stelle „von oben nach unten" durchgesetzt werden können. Die Implementierung müsse daher in erster Linie mittels Kooperationsvereinbarungen zwischen einzelnen staatlichen Ebenen erfolgen. Dies mache Erfolge schwieriger, da die erforderliche Kooperation die Komplexität der Umsetzung erhöhe.[72]

72 EU Commission 2016, S. 99 f.

Andererseits zeigt das Referenzbeispiel Österreich, das verfassungsrechtlich mit starken und autonomen Bundesstaaten ähnlich wie Deutschland organisiert ist, dass eine ausgeprägte föderale Struktur kein Hindernis für eine gelungene digitale Transformation der Verwaltung sein muss. Dort war es bereits im Juni 1998 gelungen, zwischen dem österreichischen Bundesstaat und den Bundesländern eine Kooperationsvereinbarung im Bereich Informationstechnologie zu verabschieden. Eine weitere Vereinbarung aus dem Jahr 2005 etablierte Arbeits- und Projektgruppen für die Umsetzung einer bundesweiten E-Government-Architektur. Bund, Länder sowie Gemeinde- und Städtebund konnten dafür jeweils Vertreter in diese Gruppen entsenden, die grundsätzlich auf Konsensbasis zu Ergebnissen gelangen sollten.[73]

73 Nationaler Normenkontrollrat, E-Government in Deutschland: Wie der Aufstieg gelingen kann – ein Arbeitsprogramm, 2016, *https://bit.ly/2KdS9dh*, S. 40 f.

Die Bundesrepublik Deutschland hat demgegenüber inzwischen einen etwas anderen Ansatz gewählt und anstelle einer reinen Kooperationslösung dem Bund mehr Entscheidungskompetenzen für den Aufbau der digitalen Verwaltung zugewiesen. Mit dem neuen Artikel 91 c Absatz 5 Grundgesetz hat der Bund die ausschließliche Gesetzgebungskompetenz erhalten, um den Zugang zu digitalen Behördendiensten auszugestalten. Und auch die Regelungen des OZG setzen zwar auf eine Koordinierung zwischen Bund und Ländern, zugleich wird jedoch der Schwerpunkt auf einheitliche Maßnahmen durch den Bund gelegt. So wird die Bundesregierung ermächtigt, im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung ohne Zustimmung des Bundesrats die Verwendung bestimmter IT-Komponenten verbindlich vorzugeben. Dadurch soll sichergestellt werden, dass das Bürgerportal tatsächlich in ganz Deutschland zu einer einheitlichen Plattform wird und Standards überhaupt erst möglich werden. Zudem legt das Bundesministerium des Innern, für Bau und Heimat für die Kommunikation zwischen den im Portalverbund genutzten IT-Systemen bzw. innerhalb der Verwaltung im Einklang mit dem IT-Planungsrat durch Rechtsverordnung und wiederum ohne Zustimmung des Bundesrats die technischen Kommunikationsstandards fest.

6.1.3 Datenschutz und Privatsphäre

In der Einleitung sind bereits die Gründe für die Zurückhaltung der Bürger gegenüber E-Government-Diensten beschrieben: Vielen fehlt das Vertrauen, dass ihre persönlichen Daten auf den Servern der Verwaltung sicher sind und nicht missbräuchlich verwendet werden. Zudem betonen die europäischen Leitlinien die fundamentale Bedeutung des Datenschutzes und der Privatsphäre für den Ausbau von E-Government-Architekturen, indem sie diese beiden Aspekte explizit in ihren „Prinzipien der Nutzerzentriertheit" aufnehmen.

Klar ist: Eine funktionierende digitale Verwaltung, die auf Grundsätze wie das „Once only"-Prinzip setzt, muss eine beträchtliche Menge personenbezogener Daten der teilnehmenden Bürger speichern und verarbeiten. Durch die elektronische behördenübergreifende Verfügbarkeit dieser Daten für eine unbestimmte Zahl an Verwaltungsvorgängen ist diese Speicherung auch nur unzureichend mit dem bisherigen Zustand in den Verwaltungen der Bundesrepublik vergleichbar. Natürlich sind bereits die meisten dieser personenbezogenen Daten in unterschiedlichen öffentlichen Ämtern wie dem Einwohnermeldeamt, dem Finanzamt oder der Kfz-Zulassungsstelle hinterlegt. Das hier in seinen Grundrissen konzipierte Modell eines umfassenden E-Governments jedoch baut auf der Grundidee auf, dass diese Daten an einem zentralen Ort[74] gespeichert sind, wo sie von den Bürgern verwaltet werden. Diese Daten hängen nicht nur unmittelbar mit der digitalen Identität zusammen (Name, Geburtsdatum und -ort, Meldeadresse etc.), sondern generieren im Laufe der Zeit ein Nutzungsprofil (welche Verwaltungsdienstleistungen wurden wofür genutzt), Dokumente (Geburtsurkunde, Heiratsurkunde, Grundbucheintragungen etc.), Korrespondenz mit den Behörden (elektronischer Schriftverkehr) sowie ein Logbuch darüber, wer wann welche Berechtigungen zur Datenverarbeitung erhalten hat.

74 Wenn sich auch zunächst ein Nebeneinander von zentralem Speicherort des Bürgers und den zahlreichen Registern nicht verhindern lässt.

Die Datenschutz-Grundverordnung macht für die Handhabung all dieser Daten eine Reihe von Vorgaben, die hier nicht im Detail ausgeführt werden können. Entscheidend ist jedoch, dass – insoweit nicht im Einzelfall eine spezielle gesetzliche Ermächtigung greift – die Verarbeitung der personenbezogenen Daten durch die Verwaltung nur zulässig ist, wenn der Bürger darin eingewilligt hat. Das heißt: Bei der ersten Anmeldung zum Bürgerportal muss um die klare, unmissverständliche Einwilligung gebeten werden, die Daten künftig über die Plattform verarbeiten zu dürfen. Dieser Vorgang muss insbesondere umfassende Informationen über zu erfolgendes Profiling[75] beinhalten, damit der Nutzer sich der Tragweite der Entscheidung bewusst ist, am digitalen Staat teilzunehmen.

75 „‚Profiling' […] bezeichnet die Erstellung, Aktualisierung und Verwendung von Profilen durch Sammlung von […] Daten, sowie deren anschließende Analyse und Auswertung, zum Zwecke der Identifikation und Überwachung von Personen, zur Leistungsmessung (Scoring), zur Optimierung und Vorhersage des (Direkt)marketings, oder zum Zwecke der Wahl-, Verhaltens- und Meinungsbeeinflussung" (*https://de.wikipedia.org/wiki/Profiling*).

Die Bedeutung des Grundprinzips der Einwilligung folgt nicht lediglich aus der DSGVO. Auch gemäß OZG dürfen nur mit Einwilligung des Nutzers elektronische Dokumente zu Verwaltungsvorgängen sowie Status- und Verfahrensinformationen im Nutzerkonto gespeichert und verarbeitet werden. Zudem bedarf es den gesetzlichen Bestimmungen zufolge der Einwilligung, um die Identitätsdaten dauerhaft zu speichern, sie an die für die jeweilige Verwaltungsleistung zuständige Behörde zu übermitteln sowie sie durch diese verwenden zu lassen. Authentifizierung und Autorisierung mittels der elektronischen Identität, die auf einer einmaligen Abfrage der Identitätsdaten beruht – wie oben skizziert –, ist also stets von der Zustimmung des Bürgers abhängig. Dieses Grundprinzip erstreckt sich schließlich auf die Abwicklung von Verwaltungsdienstleistungen selbst: Wie im OZG bestimmt, kann die zuständige Behörde im Einzelfall nur mit Einwilligung des Nutzers die für seine Identifizierung notwendigen Daten bei der für das Nutzerkonto zuständigen Stelle elektronisch abrufen.

Weiterhin zu nennen sind einige wichtige Betroffenenrechte, die aus der DSGVO folgen, wenn die personenbezogenen Daten eines Bürgers gespeichert sind. So ist künftig das Recht auf Auskunft über die Datenverarbeitung zu beachten. Diesem soll in dem vorgesehenen Modell dadurch Rechnung getragen werden, dass der Nutzer selbst stets die

Souveränität über die auf dem Bürgerportal hinterlegten Daten behält. Das umfasst die Möglichkeit, stets Einsicht zu nehmen, wer zu welchem Zweck auf die Daten zugreift. Zudem kann er zuvor einmal erteilte Berechtigungen auch wieder entziehen, soweit nicht zwingende rechtliche Gründe im Einzelfall dem entgegenstehen. Auf gleiche Weise wird das Recht auf Berichtigung fehlerhafter Daten über die Plattform selbst zur Geltung gebracht. Insoweit der Bürger nicht selbst Daten korrigieren kann, muss es eine Funktion geben, die es leicht und intuitiv ermöglicht, falsche Angaben zu markieren, um sie richtigstellen zu lassen. Kommt es dennoch zu Verletzungen datenschutzrechtlicher Bestimmungen während der Nutzung der E-Government-Infrastruktur, so steht dem Bürger das Recht der Beschwerde bei der zuständigen Aufsichtsbehörde zu.

Auch das viel diskutierte Recht auf Löschung bzw. „Recht auf Vergessenwerden" sollte innerhalb der E-Government-Plattform implementiert werden. Zwar enthält die DSGVO Ausnahmen von diesem Recht: Es greift beispielsweise nicht, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, welche die Verarbeitung nach dem Recht der Union oder des jeweiligen Mitgliedsstaats notwendig macht. Ein Recht auf Löschung ist auch dann ausgeschlossen, wenn die Datenverarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse liegt (Art. 17 Abs. 3 b DSGVO). Dies könnte jedenfalls auf bestimmte personenbezogene Daten oder auf bestimmte notwendige Verwaltungsvorgänge zutreffen. Davon abgesehen hat sich der deutsche Gesetzgeber im OZG dazu entschlossen, das Recht auf Löschung für E-Government jedenfalls im Grundsatz zu übernehmen. So heißt es, dass der Nutzer im Falle der dauerhaften Speicherung der Identitätsdaten jederzeit das Nutzerkonto sowie sämtliche gespeicherten Daten selbstständig löschen können muss.

All dies zeigt: Der Datenschutz ist sehr eng mit dem Prinzip der Bürgerzentriertheit verknüpft. Wenn die oben aufgezählten datenschutzrechtlichen Grundsätze beachtet werden, dann ist nicht nur rechtliche Konformität gewährleistet. Auch die Nutzungserfahrung wird positiv beeinflusst. Das Gefühl der Kontrolle über die eigenen Daten, also das Bewusstsein tatsächlicher Datensouveränität, baut Hemmnisse ab und führt zu Vertrauen und Offenheit gegenüber E-Government.

6.1.4 Regelungen über Vertrauensdienste

Auch aus der seit Juli 2016 in der Europäischen Union anzuwendenden Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS-Verordnung – „electronic IDentification, Authentication and trust Services") lassen sich rechtliche Rahmenbedingungen für den Aufbau von E-Government-Infrastrukturen in Deutschland ableiten. Hauptsächlicher Anlass für die Verordnung war das Ziel, das Vertrauen in elektronische Transaktionen zu stärken. Das Gesetz soll als umfassende Basis für die sichere elektronische Interaktion zwischen Bürgern, Unternehmen und der öffentlichen Verwaltung dienen. Es kommt immer dann zur Anwendung, wenn es um elektronische Identifikationssysteme und sogenannte Vertrauensdiensteanbieter innerhalb der Europäischen Union geht.

Ein Kernziel der eIDAS-Verordnung ist die Etablierung einheitlicher Standards für sichere elektronische Identifikation in ganz Europa. Daher macht sie Vorgaben, wie solche Systeme auszugestalten sind. Entsprechend erklären die Minister der EU- und EFTA-Staaten in der Tallinn Declaration, dass sie ihre digitalen öffentlichen Verwaltungsdienste im Einklang mit den eIDAS-Vorgaben ausgestalten, um höchsten Sicherheitsstandards zu genügen.[76] Die in Deutschland mit dem elektronischen Personalausweis und dem elektronischen Aufenthaltstitel eingeführte eID-Funktion erfüllt die Voraussetzungen bereits.[77]

76 Tallinn Declaration 2017, S. 5.

77 Vgl. *https://bit.ly/2LJLzkr.*

Die eIDAS-Verordnung regelt zudem die Anforderungen an qualifizierte und nicht qualifizierte Vertrauensdienste. Das sind insbesondere elektronische Signaturen und Siegel, die von den Vertrauensdiensteanbietern erbracht werden.[78] Eine staatliche Aufsichtsstelle überprüft, ob die qualifizierten Diensteanbieter die besonderen Sicherheitsanforderungen nach der eIDAS-Verordnung erfüllen, und erlaubt im Falle eines positiven Bescheids das Führen eines speziellen EU-Vertrauenssiegels für qualifizierte Vertrauensdiensteanbieter. Dies ist für die digitale Transformation der Verwaltung insofern in besonderem Maße relevant, als insbesondere elektronische Signaturen das Entfallen des (analogen) Schriftformerfordernisses in der Korrespondenz zwischen Behörde und Bürgern bzw. Unternehmen und damit ein rein digitales Abwickeln vieler Verwaltungsdienstleistungen erst ermöglichen.

78 Theresa Vogt, „Die neue eIDAS-Verordnung – Chance und Herausforderung für die öffentliche Verwaltung in Deutschland", Information. Wissenschaft & Praxis 2016; 67(1), *https://bit.ly/2v8rIB3*, S. 61, 62.

6.1.5 Behördlicher Datenaustausch

Ein rechtliches Problem, das sich bislang als ernstzunehmendes Hindernis für den weiteren Ausbau von E-Government-Infrastrukturen in Deutschland erwiesen hat, ist das der Regelungen zum Datenaustausch zwischen Behörden. Bislang dürfen Behörden einander nicht einfach Daten zusenden – es sei denn, es existiert eine ausdrückliche gesetzliche Grundlage für den Vorgang.[79] Das ist vor dem Hintergrund des Ziels, das „Once only"-Prinzip als tragenden Grundsatz des E-Governments zu implementieren, problematisch. Denn solange der Datenaustausch nicht vereinfacht wird, werden Bürger auch weiterhin die personenbezogenen Daten, die für eine bestimmte Verwaltungsdienstleistung benötigt werden, mehrfach eingeben und an verschiedenen öffentlichen Stellen hinterlegen müssen. Dies geht auf Kosten der Bequemlichkeit und Nutzerfreundlichkeit. Zudem senkt es vermutlich das subjektive Sicherheitsgefühl in Bezug auf die persönlichen Daten, was wiederum Vertrauensverluste zur Folge haben kann.

79 Sebastian Stern et al., „Digitalisierung 2022 – Was jetzt zu tun ist", innovative Verwaltung, 2018, *https://mck.co/2AyOlnc.*

Damit insbesondere Basisdaten, die immer wieder benötigt werden – wie Name, Geburtsort und -datum, Meldeadresse –, nicht immer wieder neu mitgeteilt werden müssen, sondern für alle Verwaltungseinheiten verfügbar sind, braucht es ein Registermodernisierungsgesetz, das die Verknüpfung der einzelnen Register gestattet.[80] Sofern der Bürger der Verbindung der eigenen personenbezogenen Daten zustimmt, könnte ein solches Gesetz den notwendigen rechtlichen Rahmen schaffen, der den Austausch zwischen Behörden für sämtliche Verwaltungsdienstleistungen erlaubt.[81] Ohne diesen legislativen Schritt ist das „Once only"-Prinzip kaum zu realisieren.

80 Henrike Roßbach und Dietrich Creutzburg, „Nie wieder Geburtsurkunden einreichen", FAZ, 6. Oktober 2017, *https://bit.ly/2006g8s.*

81 Sebastian Stern et al., 2018.

6.2 Politische Herausforderungen

6.2.1 Vorbereitung der Bevölkerung

Die Umsetzung von E-Government-Vorhaben in Deutschland ist eingebettet in eine europaweite Transformation, auf die sich die Mitgliedsstaaten von EU und EFTA gemeinsam verständigt haben. Sowohl das „Ob" als auch das „Wie" hiesiger Projekte sind damit auch von Vorgaben und Leitlinien abhängig, die außerhalb der Bundesrepublik formuliert werden, und nicht vollständig frei in der Ausführung. Trotzdem gilt es, speziell auf Deutschland zugeschnittene Lösungen zu finden, die die relevanten privaten und öffentlichen Stakeholder dort abholen, wo sie sind, und Befürchtungen und Bedenken mit umsichtiger politischer Kommunikation abzufedern.

Bereits umgesetzte Projekte wie De-Mail oder der elektronische Personalausweis haben gezeigt, dass digitale Infrastrukturen nicht allein schon deshalb von den Bürgern angenommen werden, weil sie verfügbar sind. Insbesondere dort, wo datenschutzrechtliche Fragestellungen berührt werden, gibt es in Deutschland Abwehrreflexe. Die Angst davor, was mit den eigenen personenbezogenen Daten in der digitalen Sphäre eigentlich passiert oder passieren könnte, ist oft diffus und auch durch fehlendes Wissen bedingt. Hier muss frühzeitig umfassend und transparent aufgeklärt werden. Imagekampagnen in den gängigen Medien sowie weitere Informationen mit gestaffelter Detailtiefe (ausführliche Broschüren, sehr detaillierte Erklärungen auf eigens kreierten Webseiten) können die Ängste der Bürger adressieren. Letztlich sollte ein realistisches und zugleich positives Bild vom E-Government etabliert werden: Es bietet eben nicht nur Chancen, Verwaltungsangelegenheiten schneller und bequemer zu erledigen; die Nutzer haben echte Souveränität über ihre Daten.

6.2.2 Notwendige Neuausrichtung der ausführenden Akteure

Als entscheidende politische Voraussetzung muss die Vorbereitung der einzelnen Behörden und ihrer Mitarbeiter auf die digitale Transformation gesehen werden. Die Einführung der E-Government-Architektur ist eine Aufgabe für alle Teile der Verwaltung. In den Worten des damaligen Bundesinnenministers Thomas de Maizière:

„Es wird nicht gelingen, wenn ein paar IT-Nerds dem Rest der Verwaltung Digitalisierung beibringen wollen. Man braucht die Spezialisten. Aber die gesamte Verwaltung muss sich auf digitale Prozesse einstellen. Ich denke: Ohne eine gute Qualifizierung wird es keine Digitalisierung geben – das gilt in der Wirtschaft und das gilt auch für die Verwaltung und alle ihre Beschäftigten."[82]

Entscheidend wird sein, die Belegschaften der Behörden davon zu überzeugen, die Digitalisierung als Chance für eine echte Transformation zu begreifen. Es muss gefragt werden,

82 Rede des Bundesinnenministers Dr. Thomas de Maizière anlässlich des Zukunftskongresses Staat und Verwaltung 2017, 20. Juni 2017, *https://www.bmi.bund.de/SharedDocs/reden/DE/2017/06/zukunftskongress.html.*

was die Verwaltungsmitarbeiter als Teil des Staats durch den Aufbau von E-Government-Strukturen grundlegend besser machen können als zuvor: Welche Prozesse können auf welche Weise beschleunigt werden?

Die bestehende Belegschaft benötigt ein frühes und von allen Beteiligten ernstgenommenes Veränderungsmanagement. Einerseits erscheint es notwendig, das Arbeitsumfeld innerhalb der Verwaltung dahingehend umzubauen, dass es den Raum für die für die neuen digitalen Prozesse notwendige Kreativität schafft. Andererseits wird es verstärkt darum gehen – wie bereits von de Maizière angemerkt –, die Mitarbeiter in den Behörden zu schulen und hinsichtlich der digitalen Technologien stetig weiterzubilden. Ihnen muss deutlich gemacht werden, dass sich ihre Beschäftigungsmodalitäten durch die digitale Transformation grundlegend ändern werden. Die Vorteile sind herauszustellen: Richtig implementiert und eingesetzt, bedeutet Digitalisierung, dass iterative Verwaltungsprozesse effizienter gestaltet und verschlankt werden. Dies setzt Ressourcen frei, die bei der Betreuung oder Beratung von Bürgern besser eingesetzt sind.

6.3 Gesellschaftliche und ethische Herausforderungen

Im Blick zu behalten ist schließlich eine Reihe gesellschaftlicher und ethischer Herausforderungen, die hier nur kurz angeschnitten werden können.

6.3.1 Aufbau von Vertrauen und Befähigung der Bürger

Die Herausforderung mangelnden Vertrauens innerhalb der Bevölkerung zieht sich wie ein roter Faden durch die Studie. Die Gründe hierfür sind nicht nur dort zu verorten, wo durch Unternehmen oder den Staat verursachte Datenschutzskandale unmittelbar dazu geführt haben, dass vorhandenes Vertrauen untergraben wurde. Vielmehr kann fehlende Sicherheit im Umgang mit digitalen Technologien schlicht dazu führen, dass Bürger im Zweifelsfall E-Government-Angebote nicht mehr nutzen. Laut einem Gutachten der Expertenkommission Forschung und Innovation vom 15. Februar 2017 ist die Bevölkerung in Deutschland im Umgang mit digitalen Technologien und Daten weniger erfahren als die Menschen in anderen Ländern.[83]

Die Bürger sollten also in erster Linie befähigt werden, die Dienste sicher zu nutzen. Es bedarf einer entsprechenden Fortbildung und Befähigung, beispielsweise durch attraktive und niedrigschwellige Kursangebote, sowie darüber hinaus einer besonders ausführlichen und leicht verständlichen Erklärung zur Nutzung auf den Webseiten der Dienste.

Parallel zu diesen Maßnahmen ist zudem eine verbesserte digitale Bildung der Bevölkerung in Deutschland insgesamt notwendig.[84] Vor diesem Hintergrund bedarf es einer breiten Förderung entsprechender Kompetenzen im Umgang mit Daten und digitalen Technologien.

83 Expertenkommission Forschung und Innovation, Gutachten zu Forschung, Innovation und technologischer Leistungsfähigkeit Deutschlands, Gutachten 2017, *https://bit.ly/2LXb6FW.*

84 Ebd., S. 28.

6.3.2 Transformation unter weitestgehendem Erhalt der Stammbelegschaft

Wie bereits erörtert, sollte sich die digitale Transformation auch für die Behörden selbst und ihre Belegschaft vorteilhaft auswirken. Die Mitarbeiter sollten von Beginn an einbezogen und fortlaufend ausgebildet werden. Dennoch wird die Sorge bleiben, mit der Digitalisierung könnte sich die Zahl der Bediensteten verringern. Dieser Sorge kann nur mit Aufklärung, Fakten und aufbauenden, zukunftsweisenden Maßnahmen begegnet werden.

Daher müssen die Angestellten der Verwaltung gestaltend in die Transformationsphase eingebunden werden, um ihr Wissen zu teilen und neues notwendiges Wissen aufzunehmen. Nachfolgende Maßnahmen können zur Reduktion überflüssig gewordener Rollen innerhalb der Verwaltung führen. So werden zwar nicht alle Rollen gleich bleiben, jedoch die meisten sich gemeinsam mit den Bediensteten transformieren und erneuern:

- Umschulungen: Verwaltungsangestellte sind im Umgang mit dem Bürgerportal zu schulen. Sie können anschließend als Multiplikatoren fungieren und auf öffentlichen Veranstaltungen Bürgern die Nutzung des Portals erklären. Auf diesem Wege können sie sich proaktiv auf marginalisierte Gruppen konzentrieren, wie Senioren, Migranten, Menschen aus bildungsferneren Schichten.
- Service: Geschulte Verwaltungsangestellte können über Online-Seminare („Webinare") Bürger bei der Nutzung des Bürgerportals unterstützen.
- Gemeinsame und interdisziplinäre Entwicklung der Transformation (wie oben beschrieben)
- Neue Rolle im Amt: Die digitale Transformation bietet die Chance, die Angestellten von der angestammten Rolle als Sachbearbeiter zum Berater der Bürger werden zu lassen. Durch effizienteres Zeitmanagement digitaler Technologien werden die Angestellten mehr Zeit zur Verfügung haben, um den Nutzern des Bürgerportals mit Rat zur Seite zu stehen.

6.3.3 Weitere ethische Herausforderungen

Einzugehen ist schließlich auf mögliche ethische Konflikte beim Aufbau von E-Government-Strukturen. Die vorrangige Frage ist, ob durch den Ausbau des E-Governments bestimmte Bevölkerungsgruppen oder -schichten zurückgelassen werden.

Gefährdet in dieser Hinsicht sind insbesondere Menschen, die nicht die finanziellen Mittel aufbringen können, um am E-Government teilzunehmen: etwa weil sie sich keinen Computer zu Hause oder keinen Internetzugang leisten können. Gleiches gilt für sonst sozial marginalisierte Gruppen sowie für Personen, die zwar über ausreichend finanzielle Mittel für einen Internetzugang verfügen, jedoch in Regionen leben, wo die Infrastruktur in dieser Hinsicht nicht genügend ausgebaut ist. Schließlich fühlen sich möglicherweise ältere Menschen oder solche mit bestimmten Behinderungen nicht in

der Lage, mit dem Fortschritt im digitalen Staat mitzuhalten. All diese Gruppen dürfen nicht zurückgelassen werden.

Hier gilt es, von staatlicher Seite rechtzeitig gegenzusteuern und vor allem stets einen alternativen Zugang zu Verwaltungsdienstleistungen offen zu halten. Wie das funktionieren könnte, zeigt Dänemark. Dort ist die digitale Abwicklung von Verwaltungsdienstleistungen zwar im Normalfall inzwischen verpflichtend. Es gibt allerdings Ausnahmen: So sind die Behörden vom Gesetz her verpflichtet, den „digital Abgehängten" in den kommunalen Gemeindezentren Hilfe zu leisten, beispielsweise mittels bereitgestellter Terminals in den Ämtern, also PCs, die die Bürger vor Ort nutzen können, um ihre Verwaltungsangelegenheiten dort kostenfrei digital zu erledigen. Ist ein Bürger zudem aus bestimmten Gründen überhaupt nicht in der Lage, das Bürgerportal zu nutzen, so bleibt der dänische Staat weiterhin verpflichtet, Alternativen zur Verfügung zu stellen.[85]

85 Danish Agency for Digitisation, „We Are Working to Make E-Government in Denmark More User-Friendly", 12. Februar 2014.

7 ÜBERGREIFENDE RISIKEN DER DIGITALEN TRANSFORMATION

Die vorangegangenen Abschnitte haben sich auf die Aspekte der Umsetzung einer E-Government-Architektur in Deutschland konzentriert, die um sichere digitale Identitäten als notwendiger Kern herum gebaut ist. Die Vorteile einer solchen Infrastruktur für Bürger, Unternehmen und die Verwaltung selbst wurden herausgearbeitet. Allerdings sollte – von den im sechsten Kapitel skizzierten Herausforderungen abgesehen – beachtet werden, dass der Ansatz des digitalen Staats fundamentale Risiken birgt, die auch die beste Technologie nur bis zu einem gewissen Grad abzufangen vermag.

Einerseits kann ein Übermaß an Vertrauen in digitale Infrastrukturen die Verwundbarkeit demokratischer Staatsstrukturen erhöhen. Einige Ereignisse der vergangenen anderthalb Jahrzehnte haben gezeigt, welche Folgen ein Angriff ausländischer Akteure – seien sie staatlich oder nicht staatlich – auf Kritische Infrastrukturen, die ans globale Netz angeschlossen sind, haben kann. Von den Cyber-Angriffen auf sämtliche für das Funktionieren des Staats entscheidenden Netzwerke in Estland im Jahr 2007[86] bis zu den gezielten Wählerbeeinflussungen im Präsidentschaftswahlkampf in den Vereinigten Staaten im Jahr 2016[87] ist deutlich geworden, dass die Digitalisierung insbesondere in modernen demokratisch und rechtsstaatlich verfassten Staatsstrukturen zu unkalkulierbaren Sicherheitsrisiken führen kann. Dies ist keine rein theoretische Erwägung: Auch die demokratischen Institutionen der Bundesrepublik Deutschland selbst sind bereits Ziel solcher Angriffe geworden, mit bislang nicht eindeutig abschätzbaren Konsequenzen.[88] Andererseits könnte eine für die Bürger erzwungene Digitalisierung dazu führen, dass sich

86 Vgl. Wikipedia, Internetangriffe auf Estland 2007, *https://de.wikipedia.org/wiki/Internetangriffe_auf_Estland_2007.*

87 Johannes Kuhn, „Manipuliert, mit Grüßen aus Sankt Petersburg", sueddeutsche.de, 2. November 2017, *https://www.sueddeutsche.de/digital/propaganda-im-us-wahlkampf-manipuliert-mit-gruessen-aus-st-petersburg-1.3732249.*

88 Jannis Brühl und Hakan Tanriverdi, „Was Sie über den Hackerangriff auf das Regierungsnetz wissen müssen", sueddeutsche.de, 1. März 2018, *https://bit.ly/2MbB0CX.*

diese in ihrer Identität gegenüber dem Staat zunehmend auf eine Rolle als bloße Summe von Informationen und Daten reduziert sehen. Der verringerte persönliche Kontakt mit den Mitarbeitern in den Ämtern mag bequemer sein, könnte aber zu einer schleichenden Entfremdung der Bürger von „ihrem" Staatsapparat führen, was sich wiederum negativ auf das Zusammenleben in der auf demokratischen Prinzipien basierenden Gesellschaft auswirken kann.

Aus beiden Erwägungen folgt daher: Ein direkter Kontakt zwischen Bürgern und der Verwaltung wird auch zukünftig notwendig bleiben. Persönlich zum Amt zu gehen und dort die eigenen Belange zu besprechen, muss weiterhin möglich sein. Dies sollte auch außerhalb von Notfällen oder in Angelegenheiten, die komplexere Ermessensentscheidungen seitens der Behörde erfordern, jeder Person offenstehen.

Dahinter steht der grundsätzliche Gedanke, dass E-Government kein Selbstzweck ist, sondern ein Mittel, um die Verwaltung effektiver, bürgerfreundlicher und effizienter zu gestalten. Der Einsatz von Technologie kann ungewollt das Gegenteil zur Folge haben, wenn das Fehlen menschlicher Interaktion eine Barriere schafft. Die Technik kann die menschliche Interaktion nicht ersetzen, sondern – falsch eingesetzt – bestehende Probleme sogar verschärfen. Zugespitzt gesagt: In Zeiten, in denen es in Sri Lanka einen Minister zur Bekämpfung der Einsamkeit gibt,[89] kann es nicht sinnvoll sein, sämtliche Dienstleistungen, die sonst auf dem Zusammenspiel zwischen Personen beruhen, komplett durch Technik zu ersetzen. Es muss Alternativen geben, auch weil Systeme aufgrund von Angriffen oder durch sonstige Störungen ausfallen können.

89 Ceylan Yeginsu, „U.K. Appoints a Minister for Loneliness New York Times, 17. Januar 2018, *https://nyti.ms/2Dpq5Eo*.

Dem Prinzip der Bürgerzentriertheit folgend lautet das Fazit: Es sollte stets ein alternativer Zugang zur Verfügung stehen, den Bürger wählen können, sollten sie das Bürgerportal nicht nutzen können oder wollen.

8 SCHLUSSFOLGERUNGEN ZUR ZUKUNFT DES E-GOVERNMENTS

Die Studie hat gezeigt, dass erfolgreiches E-Government in Deutschland von einer Reihe ineinander verzahnter Faktoren abhängt. Dazu gehört in erster Linie eine weitsichtige und kluge Planung, welche die bereits vorhandenen und wertvollen Verwaltungsstrukturen offline und online berücksichtigt und von Beginn an bei der Umsetzung des Vorhabens einbezieht. Die vorhandenen Ressourcen sind schon aus ökonomischen Erwägungen möglichst vollständig zu nutzen.

Ein solches Vorgehen verhindert eine Disruption der Verwaltungsstrukturen, die unabsehbare Kollateralschäden zur Folge haben könnte. Anstelle eines grundlegenden Neuentwurfs

geht es um ein intelligentes, iteratives Vorgehen, das möglichst viele Stakeholder mitnimmt – gerade auch innerhalb der Verwaltung selbst. Dazu gehört auch der schnelle Aufbau von internem Know-how: Denn auch ein Auslagern von Projekten setzt umfassende interne Expertise voraus, und zwar erstens über die einzusetzenden Technologien selbst, zweitens über die möglichen Optionen in Bezug auf die Umsetzung sowie drittens über eine realistische Einschätzung von Zeit und Kosten.

Während der Umsetzung ist bei jedem einzelnen Schritt der wegweisende Ansatz der Bürgerzentrierung zu bedenken: Der Bürger behält stets die Datensouveränität; er erteilt und entzieht, je nach Bedarf, Zugriffsrechte – Behörden und gegebenenfalls anderen dem Grunde nach berechtigten Akteuren, die im konzipierten Modell auch aus der Privatwirtschaft kommen können. Insbesondere diese Bürgerzentrierung des E-Governments hat eine Technologie für sichere digitale Identitäten zur Voraussetzung, als Dreh- und Angelpunkt für sämtliches Handeln der Bürger in der digitalen Sphäre.

Wie im Detail begründet, ist der Staat geeignet, diese Technologie zumindest teilweise selbst oder in enger Zusammenarbeit mit Dritten zu entwickeln und den Bürgern bereitzustellen. Der Grund dafür liegt in seiner besonderen Vertrauensposition. Zusätzlich zur sicheren digitalen Identität sind die Möglichkeit einer nachgelagerten Authentifizierung sowie das Prinzip des Single Sign-on von entscheidender Bedeutung. Sie sind als Teil der unerlässlichen Infrastruktur des E-Governments in Deutschland zu entwickeln. Diese Infrastrukturelemente sind den Bürgern kostenfrei zur Verfügung zu stellen. Nur so kann verhindert werden, dass Bürger auf unsichere Drittanbieter zurückgreifen.

Impressum

Zukunft E-Government
Vorschläge für eine bürgerfreundliche und
sichere Digitalisierung der Verwaltung

Herausgeber (V. i. S. d. P.)/ Verleger
(zugleich Inhaber ausschließlicher Nutzungsrechte)
Bundesdruckerei GmbH
Antonia Maas
Kommandantenstraße 18
10969 Berlin
Tel.: +49 (0)30 2598-0
E-Mail: info@bdr.de
www.bundesdruckerei.de
AG Berlin-Charlottenburg HRB 80443
USt.-Id.-Nr.: DE813210005

Projektleitung und Ansprechpartner
Bundesdruckerei GmbH
Patrick von Braunmühl
Jonas Kotzott

iRights.Lab
Philipp Otto
www.irights-lab.de

Redaktion
Wiebke Glässer

Autoren
Ramak Molavi
Henning Lahmann

Lektorat
Julia Schrader
Marc Thylmann
Textklinik® GmbH, Düsseldorf

Gestaltung
Tom Leifer Design GmbH, Hamburg

Ort und Jahr der Veröffentlichung
Berlin, Dezember 2018

Bundesdruckerei GmbH
Kommandantenstraße 18 10969 Berlin
Tel.: +49 (0)30 2598-0 Fax: +49 (0)30 2598-2205
info@bdr.de www.bundesdruckerei.de