Kapitel 1

# NEUER UMGANG MIT DIGITALEN DATEN

## Zwischen Selbstbestimmung, Freiheit und Verantwortung

—

## Effizienz in der Datenaufbereitung

V. Wittpahl (Hrsg.), *Digitalisierung*,
DOI 10.1007/978-3-662-52854-9_1, © Der/die Autor(en) 2016

Quellenangaben: Anhang, 4.2 Quellenverzeichnisse der Zahlen und Fakten

*2019 wird der mobile Datenverkehr in Deutschland monatlich ein Volumen von* **259,8 Petabyte** *erreichen – das entspricht etwa* **272 Millionen Gigabyte**. *Datensicherheit ist für insgesamt* **78 Prozent** *der Unternehmen bei der Nutzung von Cloud Computing ein Risikofaktor.* **64.426 Fälle** *von Cyberkriminalität zählte das BKA 2013 in Deutschland. Die Datenmenge, die im Jahr 2020 weltweit erstellt, vervielfältigt und konsumiert wird, wird auf etwa* **40 Zettabytes** *geschätzt. Das Speichervolumen eines menschlichen Gehirns wird auf* **2,5 Petabyte** *geschätzt. Nur* **44 Prozent** *des Webtraffics gehen direkt auf menschliche Aktivitäten zurück.*

1 Zetta = 1.000.000 Peta = 1.000.000.000 Tera = 1.000.000.000.000 Giga

# ZWISCHEN SELBSTBESTIMMUNG, FREIHEIT UND VERANTWORTUNG

## Die Chance der digitalen Souveränität

*Joachim Lepping, Matthias Palzkill*

—

## IT-Sicherheit und Nutzer: Chancen und Risiken in der Digitalisierung

*Stefan G. Weber*

## 1.1.1 Die Chance der digitalen Souveränität

*Joachim Lepping, Matthias Palzkill*

*Durch die zunehmende Vernetzung aller Lebensbereiche steigt die Abhängigkeit von digitalen Infrastrukturen, mit denen Bürgerinnen und Bürger täglich in Interaktion treten. Angeboten werden diese Infrastrukturen vorrangig von internationalen Konzernen, die so dynamisch agieren können, dass sie sich in wirtschaftlicher und datenschutzrechtlicher Hinsicht künftig nationalstaatlichen Regulierungen entziehen. Daher ist zum einen das souveräne Handeln der einzelnen Bürgerinnen und Bürger bedroht. Zum anderen sieht sich eine digitalisierte Industrie durch zunehmende Angriffe und verstärkte Abhängigkeiten von internationalen Technologielieferanten in ihren Handlungsoptionen eingeschränkt. Der vorliegende Beitrag erläutert Maßnahmen zur Stärkung der Souveränität Deutschlands und Europas auf individueller, organisationaler und gesellschaftlicher Ebene. Darüber hinaus werden die durchaus zahlreich vorhandenen Potenziale und Chancen für die Bewahrung der digitalen Souveränität Deutschlands aufgezeigt.*

Gibt es heute Abend noch freie Plätze in der Oper? Ist der aktuelle Dave Eggers-Bestseller momentan in der Stadtbibliothek verfügbar? Wann wird mein Paket geliefert? Wo finde ich in der Altstadt gerade einen freien Parkplatz, und wie gelange ich am schnellsten dorthin? Diese und ähnliche Alltagsfragen werden zunehmend durch digital vernetzte und gesteuerte Systeme beantwortet. Social-Media-Plattformen, Onlinebanking, individualisierte Produktion bis hin zu telemedizinischen Anwendungen zeigen:

Die Digitalisierung der Gesellschaft ist bereits Realität und Daten sind der digitale Treibstoff, der diesen weltweiten Dienstebetrieb in Gang hält.

Der Begriff „Digitale Souveränität" beschreibt einen Zustand im Spannungsfeld von Fremdbestimmtheit und Autarkie über Erhebung, Übertragung, Verarbeitung und Speicherung von Daten (Abbildung 1.1.1.1: Ebenen der digitalen Souveränität). Hierbei gilt es abzuwägen, welches Maß an Selbstbestimmung im Einzelfall gewünscht, sinnvoll oder möglich ist. Nur so gelingt der notwendige Spagat zwischen Gesetzgebung und technischen Aspekten. Letztlich geht es in der immer lebhafter werdenden Debatte um nichts weniger als die Neuverhandlung der Machtgrenzen zwischen Staaten, ihren Bürgern und einer globalisierten Wirtschaft. Im Mittelpunkt muss hierbei die Frage stehen, welchen unaufhaltsamen Gesetzmäßigkeiten die Digitalisierung unter-


*Abbildung 1.1.1.1: Ebenen der digitalen Souveränität*

liegt und welche Gestaltungsmöglichkeiten, Handlungsspielräume und wirtschaftlichen Chancen sich aus dem Ziel der Schaffung von digitaler Souveränität ergeben.

### *Die digitale Welt von heute*

Durch die zunehmende Vernetzung nahezu aller Lebensbereiche werden Bürgerinnen und Bürger stetig abhängiger von digitalen Infrastrukturen, Dienstleistungen, Endgeräten und Datenquellen, mit denen sie täglich interagieren. Dabei reizt vor allem das erhebliche Potenzial zur Effektivitäts- und Effizienzsteigerung, welches die Digitalisierung in allen Lebensbereichen bietet. Ebenso eröffnen sich individuelle Handlungsmöglichkeiten, die vormals – wenn überhaupt – nur großen Organisationen mit erheblichem Aufwand vorbehalten waren. Hierzu zählen gestalterische Möglichkeiten wie die Verbreitung von Informationen, aber auch zerstörerische Handlungen wie Manipulationen oder Datendiebstahl.

Geschwindigkeit und Ausmaß digitaler Transformationen führen naturgemäß zu disruptiven Veränderungen, welche sowohl Aufbruchsstimmung als auch Abschottungswünsche hervorbringen. Daher ist es wichtig, die zugrundeliegende Gesetzmäßigkeit in diesem Rahmen zu verdeutlichen: Die Digitalisierung folgt dem Bacon'schen Diktum „Wissen ist Macht". In der Folge sind, wie von Bundeskanzlerin Merkel betont, „Daten der Rohstoff des 21. Jahrhunderts" und somit in einer zukunftsfähigen Produktion (Industrie 4.0) das zentrale Element, um Optimierungen und damit Profitmaximierung zu erreichen (CeBIT 2016). Das Nutzen möglichst vieler Daten zur Erzielung höherer Unternehmensgewinne folgt dabei dem Grundprinzip einer markt-

wirtschaftlichen Wirtschaftsordnung. Es gilt sich darüber im Klaren zu sein, dass der Handel mit Daten auch in weiter Zukunft noch unser wirtschaftliches Handeln stark bestimmen wird.

### *Technologische Fremdbestimmtheit*

Wesentliche Bestandteile der digitalen Transformation sind die weltweite Verbreitung leistungsstarker vernetzter Endgeräte sowie der Ausbau leistungsstarker Netzwerke und Ressourcen-Infrastrukturen. Problematisch jedoch ist, dass die Schnittstellen von Endgeräten wie Smartphones oder Tablets sowie die bereitgestellten Dienstleistungen hinsichtlich Datenerfassung bzw. -nutzung durch einzelne Nutzerinnen und Nutzer nur unzureichend beherrscht werden. Gleichzeitig lassen sich Betreiber durch zu akzeptierende Nutzungsbedingungen einen größtmöglichen rechtlichen Handlungsspielraum einräumen und entziehen so dem Nutzer zum Teil die Kontrolle über die erfassten Daten. Jedem Akteur muss bewusst sein, dass vermeintliche Gratis-Dienstleistungen im Internet immer mit persönlichen Daten bezahlt werden und die Nutzenden in Wirklichkeit gar nicht Kunden, sondern Zulieferer eines Geschäftsmodells sind. Wären diese Infrastrukturen und Dienste vollständig durch ein entsprechendes (z. B. nationales) Rechtssystem reguliert, könnte die digitale Souveränität jedes Akteurs durch den Gesetzgeber gewährleistet werden. Wie die Debatte um die Vorratsdatenspeicherung aber zeigt, wäre schon auf nationalstaatlicher Ebene ein heftiger demokratischer Diskurs zu erwarten, da Interessen der Bürgerinnen und Bürger, der Wirtschaft und des Staates in Konsens zu bringen sind.

Eine neue Qualität ergibt sich jedoch dadurch, dass Anbieter und Ausrüster von Endgeräten, Infrastrukturen und Diensten von internationalen Konzernen entwickelt und kontrolliert werden. Diese können so dynamisch agieren, dass sie sich sowohl in technologischer als auch in ethischer, sozialer und rechtlicher Hinsicht zunehmend nationalstaatlichen Regulierungen entziehen. Daher ist zum einen das souveräne Handeln der einzelnen Bürgerinnen und Bürger bedroht, zum anderen sieht sich aber auch die Industrie durch vermehrte Angriffe auf diese digitalen Infrastrukturen und verstärkte Abhängigkeiten von internationalen Technologielieferanten in ihren Handlungsoptionen eingeschränkt. In letzter Konsequenz sind hiervon gleichermaßen auch die politischen Systeme, die sich traditionell über ein räumlich festgelegtes Gebiet definieren, betroffen, da sich digitale Datenströme über staatliche Grenzen mehr oder weniger ungehindert hinwegbewegen.

### *Überwachte Daten*

Die Bedrohungslage wird mit steigender Digitalisierung – zumindest gefühlt – immer größer. Seit der Debatte um die Vorratsdatenspeicherung sind viele Menschen in

Deutschland für das Thema IT-Sicherheit sensibilisiert. Gleichzeitig herrscht eine Ohnmacht bezüglich konkreter Schutzmaßnahmen. In dieser Gemengelage werden Spionageaktivitäten unbekannten Ausmaßes immer einfacher umsetzbar, da de facto zahlreiche öffentliche Kommunikationsnetze bei Bedarf nutzbare Abhörschnittstellen enthalten. Auf diese Weise hat sich ein milliardenschwerer Markt von digitalen Überwachungstechnologien etabliert, der zu großen Teilen sogar über Geheimdienste staatlich finanziert wird.

Verschärft wird diese Entwicklung durch selbstlernende Algorithmen, die neben der Überwachung auch die Vorhersagbarkeit des Verhaltens von Akteuren (d. h. sowohl Bürgerinnen und Bürger als auch Unternehmen) zum Ziel haben. Diese Algorithmen können in Teilen heute bereits treffsicher entscheiden und erzeugen so eine neue Qualität der Unmündigkeit, besonders wenn sich betroffene Akteure ihrer eigenen Transparenz und Vorhersagbarkeit gar nicht bewusst sind. Diese Algorithmen zusammen mit der bewussten oder unbewussten eigenen Transparenz stellen eine zunehmende Gefahr der eigenen digitalen Souveränität dar.

### *Selbstbestimmtes Handeln*

Digitale Souveränität im Rahmen selbstbestimmten Handelns beschreibt die Fähigkeit, die Vertrauenswürdigkeit, Integrität und Verfügbarkeit der Datenverarbeitung durchgängig kontrollieren zu können. Idealerweise kann sichergestellt werden, dass keine technischen Mittel im Kommunikationsnetzwerk vorhanden sind, die unberechtigten Zugriff, Veränderung oder Weiterleitung der Daten zulassen. Digitale Souveränität bemisst sich somit durch den Grad der Selbstbestimmtheit und der Kontrolle über die jeweiligen Glieder der Datenkette: Erhebung, Übertragung, Verarbeitung und Speicherung.

Grundlage der digitalen Souveränität ist es, Akteure zu einer bewussten Entscheidung zu befähigen, sodass sie Risiken einschätzen und über das Schutzniveau ihrer Datenkommunikation bedarfsgerecht entscheiden können. Hierbei handelt es sich um eine gesamtgesellschaftliche Aufgabe, die Handlungsfelder nicht nur im Bereich der IT-Sicherheit, sondern beispielsweise auch in wesentlichen Technologiebereichen der deutschen Wirtschaft wie der Automobilindustrie oder der Energietechnik schafft. Der Wirtschaft und Gesellschaft muss es möglich sein, digitale Technologien so zu nutzen, dass zum einen Datenschutzinteressen nicht beeinträchtigt, zum anderen darauf aufbauende wirtschaftliche Verwertungs- und Geschäftsmodelle umsetzbar sind. Darüber hinaus müssen sich wirtschaftliche Entwicklungen im Bereich der IKT ungehindert realisieren und im internationalen Markt vertreiben lassen.

### *Die digitale Welt von morgen*

Die Strukturen des Internets unterliegen einem permanenten Entwicklungsprozess. Neue Anwendungsmöglichkeiten ergeben sich durch die flexible Bereitstellung von Ressourcen (Cloud Computing), die Integration bisher IT-ferner Komponenten (Internet der Dinge) und die Erfassung und Verknüpfung noch größerer Datenmengen (Big Data). Dabei herrscht ein engagiert geführter weltweiter Konkurrenzkampf um Technologieführerschaft, Innovationsvorsprünge, Marktzugänge und Beherrschung von aktuellen und künftigen digitalen Absatzmärkten. Neben den Anbietern von Basistechnologien etabliert sich ein Wettstreit um den Absatz von Diensten, die sich die Daten und Infrastrukturen zunutze machen. Die Profiteure des digitalen Wandels sind daher vermutlich in ganz neuen Geschäftsmodellen zu sehen. Beispielsweise gibt es viele Start-ups, die sich auf die Vernetzung des Haushaltes fokussieren. Das inzwischen von der Alphabet Inc. übernommene Start-up Nest oder die Firma Tado aus München vertreiben Thermostate, die per App gesteuert werden können. Diese Start-ups werten umfangreiche Messdaten aus und verknüpfen diese mit ihren vernetzten Systemen, um für den Endanwender Mehrwertdienste und Optimierungen (z. B. zur Energieeffizienz) anzubieten.

Aktuelle Entwicklungen basieren auf dem Ansatz, sämtliche digitale Dienstleistungen ausschließlich bedarfsgerecht bereitzustellen (on-demand). Ohne Zweifel ein Geschäftsmodell mit unbestreitbaren Vorteilen. Dennoch: Auch die permanente Abhängigkeit des Einzelnen von globalen Unternehmen nimmt stark zu und verschärft somit die Frage nach digitaler Souveränität. Für den Kunden entfällt die Möglichkeit zum dauerhaften Kauf und somit auch zum Besitz von Produkten. Für Unternehmen wird das Modell des „Everything-as-a-Service" auf etablierte Akteure einen nie dagewesenen Anpassungsdruck erzeugen mit dem Potenzial, ganze Bestandsmärkte revolutionieren zu können.

### *Marktentwicklung*

Im Hinblick auf die digitale Souveränität Deutschlands sind folgende Feststellungen zentral und notwendig: Die Evolution des Internets wird aktuell von wenigen großen Akteuren getrieben. Mehr noch, wesentliche Teile von IKT-Systemen und der benötigten Infrastrukturebenen stammen zurzeit nicht aus Deutschland (und auch nicht aus Europa). Den IT-Bedarf in Deutschland umfassend aus der eigenen Industrie zu bedienen ist – Stand heute – unmöglich. Ähnlich ist es bei den anwenderbezogenen Internetdiensten: Auch hier erleben wir aktuell eine zunehmende Konzentration auf einige wenige große Konzerne, die einen wesentlichen Teil aller Datenströme beherrschen. Darüber hinaus arbeiten diese marktdominierenden Firmen typischerweise mit Konditionen wie dem Erlangen der Rechte an von Nutzerinnen und Nutzern

erstellten Inhalten, der Datenverarbeitung ohne Einwilligung oder fehlender Löschrechte.

Für die Debatte zur digitalen Souveränität bedeutet dies, dass sie zu einem Zeitpunkt geführt wird, zu dem zentrale technologische Bereiche Deutschlands und teilweise auch Europas nur noch als Technologiefolger eingestuft werden können. Diskutiert werden überwiegend wirtschaftspolitische Handlungsmöglichkeiten, während Maßnahmen zum Schutz der Bürgerinnen und Bürger zunächst im Umfeld der Forschungsförderung erarbeitet werden. So geht es beispielsweise in der Debatte zum „Trusted Computing" letztendlich darum, welche Funktionen auf IKT-Endgeräten, privaten Routern oder Autos erlaubt und welche verboten sind. In einem digital souveränen Staat ist es allerdings auch erforderlich, dass Eigentümer von IT-Geräten selbst die Kontrolle über ihre IT-Geräte haben. Hierfür hat Deutschland durchaus die technologischen Möglichkeiten, um durch die eigene Industrie die digitale Souveränität in vielen Bereichen herzustellen oder zu erhalten.

### *Bedarfslücken identifizieren*

Damit der Innovationsstandort Deutschland seine digitale Souveränität wiedererlangt und auch künftig wettbewerbsfähig bleibt, sind neben dem Ausbau der Internetmöglichkeiten auch Schlüsseltechnologien, insbesondere im Bereich von Soft- und Hardware, entscheidend. Um den Technologievorsprung der großen weltweiten Hersteller aufzuholen, fehlt es jedoch an Ressourcen, an der notwendigen Entwicklungszeit, aber auch der Motivation auf etablierte Suchmaschinen und soziale Netze zu verzichten. Letzteres zeigt deutlich: Weder der Weg in Richtung Isolation ist wünschenswert, noch stellt ein Verfolgen der Technologieführer langfristig die digitale Souveränität her.

### *Ökonomische Chancen nutzen*

Deutschland bleibt bei Internetdiensten derzeit nur die Rolle des „Smart Followers", der bestehende Entwicklungen aufgreifen muss und hieraus neuartige Dienste entwickelt. Auch wenn für Deutschland als Hochtechnologiestandort bisher kaum vorstellbar, bedeutet dies unter den aktuellen Rahmenbedingungen für die digitale Souveränität keinen Nachteil, sondern birgt eine vielleicht noch unbekannte Chance. Während sich die großen Infrastrukturtechnologieführer mit dem Ausbau ihrer Plattformen um jeden Preis beschäftigen, können sich Deutschland und Europa auf die Erforschung und Umsetzung langfristig tragfähiger Mehrwertdienste konzentrieren.

So ergeben sich für den Standort Deutschland Perspektiven bei Technologien und innovativen Diensten in den Bereichen Datenschutzgarantie und IT-Sicherheit. Dies schließt auch den Rechtsraum als Standortfaktor mit ein. Deutschland kann sich

(ähnlich der Attraktivität als Produktionsstandort aufgrund guter Infrastruktur und aufgrund hochqualifizierten und motivierten Personals) durch die rechtliche Verankerung eines hohen Datenschutzniveaus gepaart mit einem technologisch gestützten, verantwortlichen Datenumgang international behaupten. Die Herstellung der digitalen Souveränität der Bürgerinnen und Bürger muss als Innovationstreiber gesehen werden. Digitale Souveränität wird so zum vorrangigen wirtschaftlichen und politischen Ziel.

Strategien, als Technologiefolger zu agieren, sind nur dann erfolgreich, wenn deren Umsetzung nicht in zu großen zeitlichen Verzug gerät. Deutschland ist für diese Herausforderungen sehr gut aufgestellt. Das Land verfügt zum einen über bedarfsgerechte Forschungsförderung, zum anderen weist die Wirtschaft durch das Zusammenspiel von Großindustrie mit kleinen und mittelständischen Unternehmen allgemein ein hohes Innovationspotenzial auf. Darüber hinaus ist besonders in den Ballungsräumen eine aufblühende Start-up-Szene präsent.

Innovationspolitische Verantwortung liegt nun in erster Linie darin, vorhandene Ressourcen in strategisch wichtige Themenfelder zu investieren. Darüber hinaus sind nach wie vor innovative Technologien aus Deutschland zu erwarten. Und auch die Investition in nationale Konkurrenzprodukte lohnt sich, wenn diese Lücken im Markt schließen, beispielsweise bei kritischen Infrastrukturen, wo das Risiko eines Souveränitätsverlustes den Aufwand für eigene Entwicklungen rechtfertigt.

### *Regulatorische Rahmenbedingungen schaffen*

Der Wunsch nach einem durchgängig gewährleisteten Datenschutz und einer ausreichenden IT-Sicherheit im klassischen Sinne ist richtig und wichtig. Dies sollte aber zur Begünstigung der digitalen Souveränität durch zusätzliche Maßnahmen ergänzt werden. Als Gesellschaft müssen wir uns beispielsweise mit der Frage auseinandersetzen, warum personalisierte Werbung schlecht sein soll. Solange der Nutzungsumfang zwischen den Beteiligten fair ausgehandelt und klar definiert ist und zudem die Zweckentfremdung personenbezogener Daten verhältnismäßig sicher erkannt und gesetzlich effektiv verfolgt werden kann, sind wichtige Voraussetzungen zur digitalen Souveränität prinzipiell geschaffen.

Für ein digital souveränes Handeln sind mehrere Aspekte relevant: Es ist notwendig, Schlüsseltechnologien zu beherrschen und eine hohe Kompetenz in zentralen Technologiebereichen zu haben. Ebenso ist eine effektive IT-forensische Aufklärung von IT-Sicherheitsvorfällen und die damit einhergehende Abschreckung vor Datenmissbrauch entscheidend. Und nicht zuletzt müssen neue technologische Trends überhaupt identifiziert und eingeordnet werden, um diese dann aus eigener Kraft weiterentwickeln zu können.

### *Verantwortungsvolle Technologien befördern*

Gesamtgesellschaftlich muss Technologieentwicklung und -nutzung neu verstanden werden. Im Rahmen technologischer Innovationen müssen auch nicht-technologische Implikationen mitbedacht werden. Hierfür existieren auf nationaler und europäischer Ebene bereits integrierte Forschungsansätze. Diese Konzepte zielen darauf, nicht-technologische Aspekte technologischer Innovationen frühzeitig zu adressieren und interdisziplinär zu betrachten. Hierzu zählen ethische, soziale und rechtliche Fragestellungen, die zwangsläufig bei Technologien entstehen, die immer näher an den Menschen heranrücken. Zwischen der Verhinderung und der Gestaltung von Innovationen müssen diese Ansätze förderpolitisch weiterentwickelt und besser aufeinander abgestimmt werden. In einem gesellschaftlichen Diskurs muss dabei das hinreichende Maß digitaler Souveränität bestimmt werden.

### *Entwicklungsziele*

So wie die soziale Marktwirtschaft dem ungezügelten Kapitalismus Grenzen aufweisen kann, so muss die Digitalisierung in soziale Bahnen gelenkt werden. Aus der gesellschaftlichen und wirtschaftlichen Forderung nach Erhalt und Sicherung der digitalen Souveränität ergeben sich vielfältige technologische Chancen. Diese liegen unmittelbar in dem konsequenten Ausbau von Datenschutztechnologien und der IT-Sicherheitstechnik (Abbildung 1.1.1.2: Spannungsfeld der Selbstbestimmung). In

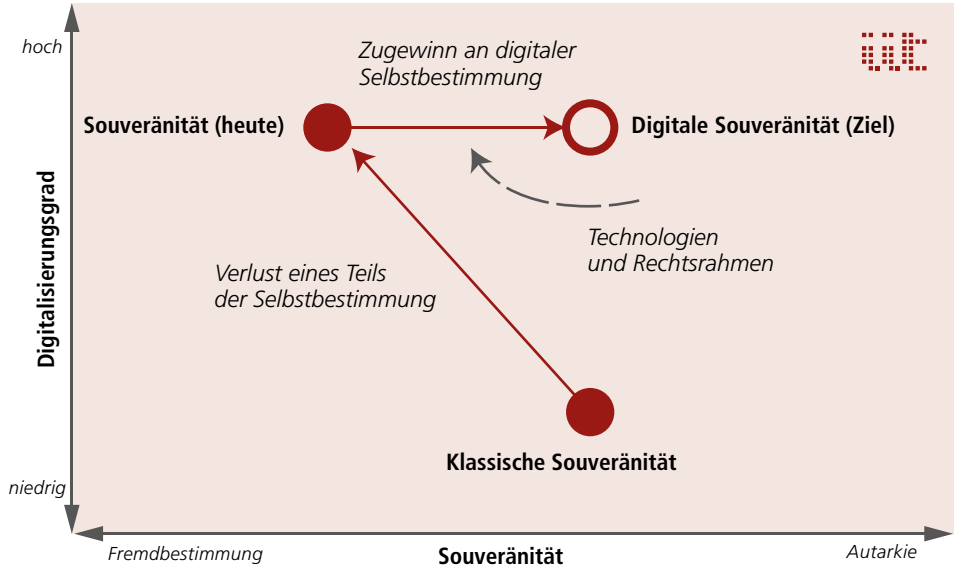


*Abbildung 1.1.1.2: Spannungsfeld der Selbstbestimmung*

Hinblick auf die benötigten Technologien für Hardware-basierte IT-Sicherheitstechnik haben Deutschland und Europa durch innovative Mikrosystemtechnik einen großen Innovationsvorsprung. Ähnliches gilt für die Technologieführerschaft im Bereich eingebetteter Software, die aus einer langen und engen Zusammenarbeit mit den Anwendungsbranchen Automobil, Produktion und Energie resultiert. Hier bestehen Chancen, die Erfahrungen aus verteilten Softwaresystemen für künftige Industrie-4.0-Produktionsanwendungen zu nutzen. Es ist somit ohne Weiteres möglich, sich dem Wettbewerb mit Unternehmen der Internet-Branche zu stellen, denen die Kompetenz in der eingebetteten Software heute fehlt.

Während in der Netzwerktechnologie und im Bereich der großen Internetdienste und -plattformen besonders US-amerikanische Konzerne die Technologieführerschaft übernommen haben, werden in Deutschland und in europäischer Kooperation Verfahren entwickelt, die einen sicheren Datentransport ermöglichen und das verschlüsselte Prozessieren von Internetdaten erlauben. Für Deutschland besteht die Möglichkeit, die Digitalisierung auf individueller, organisationaler und gesellschaftlicher Ebene mit sozialer Innovation zu verbinden. „Made in Germany" kann dann für hochwertige und verantwortungsvolle Technologien stehen, die gegenüber möglicherweise kurzlebigen Internetgiganten langfristig Bestand haben werden.

### *Literatur*

CeBIT (2016) Bundeskanzlerin Merkel: Daten sind die Rohstoffe des 21. Jahrhunderts. CeBIT News, 12.03.2016. www.cebit.de/de/news/bundeskanzlerin-merkel-daten-sind-die-rohstoffe-des-21.-jahrhunderts.xhtml. Zugegriffen: 18.05.2016

## 1.1.2 IT-Sicherheit und Nutzer: Chancen und Risiken in der Digitalisierung

*Stefan G. Weber*

*IT-Sicherheit ist eine Grundbedingung für das Gelingen der Digitalisierung. Durch die Digitalisierung scheinen sich die Verletzlichkeiten unserer Gesellschaft und Wirtschaft jedoch zu potenzieren. Dieser Artikel adressiert die Frage, welche Herausforderungen prioritär anzugehen sind, um die Bedrohungsszenarien des „gläsernen Bürgers" und der „verwundbaren digitalen Wirtschaft" abzuwenden. Neben fehlenden „digitalen Instinkten" stehen häufig auch fehlende ökonomische Anreize dem Einsatz der oft komplexen Schutzmechanismen entgegen. Der Beitrag stellt Handlungsmöglichkeiten für diese Problemfelder vor und plädiert dafür, die Digitalisierung auch als Chance für IT-Sicherheit und Datenschutz zu begreifen und die zahlreichen Chancen, welche sich für Wirtschaft und Gesellschaft ergeben, konsequent zu nutzen.*

### *Einführung*

Jede und jeder Einzelne von uns interagiert täglich im Berufs- und Privatleben mit einer Vielzahl von vernetzten, digitalen Systemen, sowohl bewusst als auch unbewusst. Die prinzipielle *Schutzbedürftigkeit* der dahinterstehenden Systeme, der zirkulierenden digitalen Informationen und nicht zuletzt der Persönlichkeitsrechte der handelnden Personen – also von uns allen – wurde vielfach festgestellt.

Nicht zuletzt ist der individuelle und kollektive *Schutzanspruch* in Deutschland auch gesetzlich verankert. Als Reaktion auf die für das Frühjahr 1983 angesetzte Volkszählung wurde etwa das Grundrecht auf informationelle Selbstbestimmung verfassungsrechtlich verankert. Schon damals galt und es gilt noch heute: Eine von Betroffenen unbeherrschbare und unbeherrschte Datensammlung und Datenverarbeitung, bedingt durch die zunehmende Verbreitung der modernen Informationstechnik, stellt eine potenzielle Gefährdung unserer freiheitlichen Grundordnung dar. Wenn der oder die Einzelne nicht mehr wissen und beeinflussen könne, von wem welche Daten mit Bezug zum persönlichen Verhalten gespeichert oder vorrätig gehalten werden, passe sie oder er sein Verhalten aus Vorsicht an, um nicht durch „abweichende" Verhaltensweisen aufzufallen – so argumentierte das Bundesverfassungsgericht (vgl. BMI 2016). Die Beeinträchtigung nicht nur der individuellen Handlungsfreiheit, sondern auch unseres freiheitlichen, demokratischen Gemeinwesens, welches einer selbstbestimmten Mitwirkung der Bürgerinnen und Bürger bedarf, durch eine entgrenzte Datener-

hebung, -verarbeitung und -weitergabe steht somit nicht erst in Zeiten der Digitalisierung zur kritischen Diskussion. Durch die Digitalisierung scheinen sich die Verletzlichkeiten unserer Gesellschaft und Wirtschaft zu potenzieren. Vor diesem Hintergrund stellt sich die Frage, welche Herausforderungen prioritär anzugehen sind, um die Bedrohungsszenarien des „gläsernen Bürgers" und der „verwundbaren digitalen Wirtschaft" abzuwenden (vgl. Kapitel 1.1.1 und Kapitel 3.1.3).

Im Folgenden werden zwei zentrale Themenbündel betrachtet:

- Digitalisierung bringt zentrale IT-Sicherheitsprobleme ans Licht
- Digitalisierung ist auch als Chance für IT-Sicherheit und Datenschutz zu denken

Dabei werden zum einen wichtige Entwicklungen aus der Forschung aufgegriffen und künftige Entwicklungen antizipiert, zum anderen werden die IT-Sicherheitsaspekte auch in einen größeren Gesamtzusammenhang eingeordnet.

### *Herausforderungen für IT-Sicherheit und Datenschutz in einer digitalisierten Welt*

IT-Sicherheits- und Datenschutzaspekte sind zentrale Querschnittsanforderungen, die bei der Digitalisierung zu berücksichtigen sind. Doch warum ist der Umgang mit IT-Sicherheit weiterhin so brisant? Nach den Enthüllungen von Edward Snowden zur flächendeckenden Massenüberwachung unserer digitalisierten Welt durch Geheimdienste wurde eine „Vertrauenskrise" in der IT-Sicherheit proklamiert.

Ein Hauptproblem liegt weiterhin in der Diskrepanz zwischen Wunsch und Wirklichkeit. Vor diesem Hintergrund lassen sich die folgenden drei zentralen Problembereiche identifizieren.

*I. Fehlende „digitale Instinkte"*

Jede und jeder von uns lernt von klein auf, welche Gefahren ein unvorsichtiges Verhalten mit sich bringt: An gefährlichen Gegenständen kann man sich verletzen, an heißen Gegenständen kann man sich verbrennen. „Auch wenn wir nachts durch den Wald gehen und es raschelt, dann werden wir sofort sehr aufmerksam und vorsichtig." (Borchers 2015)

In einer digitalisierten Welt sind neue Bedrohungslagen hinzugekommen, auf welche wir noch nicht instinktiv reagieren können. Die Gefahren beim Einsatz und der Nutzung von digitalen Technologien lassen sich auch oftmals gar nicht direkt wahrnehmen. Daher werden der Schutzbedarf sowie die möglicherweise weitreichenden, aber ggf. nur langfristigen Konsequenzen eines Datenmissbrauchs durch Dritte oft unterschätzt.

*II. Schutzmechanismen sind nicht integriert und zu komplex in der Nutzung*

IT-Sicherheitsmechanismen werden oft erst nachträglich – sozusagen als Add-on – in Systeme, Produkte und Dienste eingefügt. Sie haben somit zunächst keine unabhängige Funktion und erschweren die Nutzung von Informations- und Kommunikationstechnologien, im privaten wie im geschäftlichen Umfeld. Sie erzeugen so zunächst einen Overhead bei Geschäftsprozessen und sorgen für unnötige Komplexität bei der Nutzung, sei es bei der E-Mail-Verschlüsselung oder beim Zugriff auf das persönliche Endgerät der Wahl. Somit wird auch menschliches Verhalten, das Sicherheitsmechanismen umgeht, zu einem zentralen Angriffs- oder Schwachpunkt.

*III. Fehlende Anreize*

Neben organisatorischen Umsetzungsschwierigkeiten und Engpässen bei Fachpersonal spielen bei der Implementierung von Sicherheitsmechanismen besonders die Kosten bzw. das Kosten-Nutzen-Verhältnis eine wichtige Rolle. Warum aber sollten auf Gewinnmaximierung bedachte Firmen Daseinsvorsorge betreiben, obwohl kein direkter „Return on Investment" absehbar ist?

## *Die Suche nach Lösungsmöglichkeiten*

IT-Sicherheit muss, um auch im Alltag anzukommen, anwenderfreundlich und benutzbar und nicht zuletzt verstehbar sein. In der Forschung und auch in frühen wirtschaftlichen Umsetzungsphasen finden sich verstärkt Ansätze, welche den Problembereich II, unter Begriffen wie „Privacy by Design" (Cavoukian 2011) und „Usable Security" (Cranor und Garfinkel 2005) adressieren. Die Begriffsbildung „by Design" soll dabei andeuten, dass Datenschutz- und IT-Sicherheitsanforderungen bereits in frühen Phasen der Systemgestaltung aufzugreifen und kontinuierlich über alle Lebensphasen zu beachten sind. Für ein zunächst „sicher" konzipiertes und implementiertes System können sich beispielsweise in der Konfigurationsphase neue Schwachstellen dadurch ergeben, dass kryptographische Schlüssel über einen unsicheren Kanal kommuniziert und so unerwünschte Hintertüren geschaffen werden.

Solche und andere unerwünschten Einfallstore können vermieden werden, indem explizite Nutzerinteraktionen mit sicherheitsrelevanten Anteilen, wo möglich, vermieden werden und damit auch die Komplexität der Nutzung reduziert wird. Dieser Trend der „impliziten Sicherheit" findet sich beispielsweise in Mechanismen zur kontinuierlichen Authentifizierung wieder: Ein persönliches Endgerät kann etwa anhand des Ganges erkennen, ob der aktuelle „Träger" mit dem „Besitzer" übereinstimmt und in diesem Fall den erlaubten Zugriff freischalten (vgl. Weber 2014). Auch die Kombination verschiedener impliziter und expliziter Verifizierungsverfahren kann wesentlich zur Steigerung von Sicherheit und Benutzbarkeit beitragen (Abbildung 1.1.2.1).

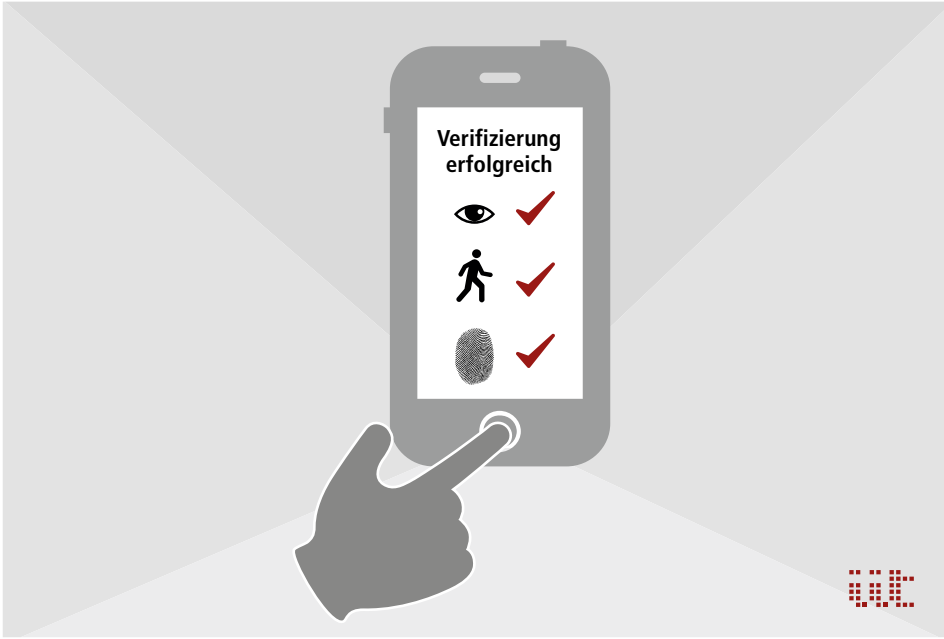


*Abbildung 1.1.2.1: Kombination impliziter und expliziter Ansätze zur Verifizierung einer Identität*

Mit der Fragestellung der fehlenden ökonomischen Anreize befasst sich die Forschung zur Ökonomie der IT-Sicherheit („economics of IT security") seit Anfang des Jahrtausends (vgl. Anderson 2001). In der Ökonomie der IT-Sicherheit werden beispielsweise Fragestellungen untersucht, warum bestimmte Angriffe und Datenschutzrisiken in Kauf genommen werden, obwohl technische Lösungen zur Verhinderung oder Abschwächung von IT-basierten Angriffen oder zur Reduzierung von Datenschutzrisiken verfügbar sind. Hierzu werden Modelle des sogenannten „rational denkenden Menschen" sowie der Verhaltensökonomie herangezogen. Aus ökonomischer Sicht ist die Frage zunächst scheinbar einfach zu beantworten: Übersteigen die erwarteten Kosten zum Schutz vor IT-Angriffen den erwarteten Schaden, der durch IT-Angriffe entsteht, ist es billiger den Schaden zu (er)tragen und keine Investitionen in Schutzmaßnahmen zu tätigen.

In der Ökonomie werden sogenannte Grenzbetrachtungen durchgeführt, die auch hier Anwendung finden. Es wird entsprechend nur so lange in IT-Sicherheitsprodukte investiert, wie jeder zusätzlich investierte Euro den erwarteten Schaden um mehr als einen Euro reduziert. Man spricht von Grenzkosten und Grenzschaden.

Aus gesamtwirtschaftlicher Sicht ist diese Betrachtungsweise durchaus korrekt, jedoch lohnt hier ein zweiter Blick. Gerade im Bereich der ökonomischen Forschung müssen die Auswirkungen auf die einzelnen Akteure differenziert betrachtet werden. Die Kosten der Schutzmaßnahmen fallen selbstverständlich direkt etwa bei den Unternehmen an, der entstandene Schaden jedoch weniger. Gelangt ein Angreifer beispielsweise in den Besitz einer Unternehmensdatenbank, die viele sensible personenbezogene Daten enthält und berichtet die Presse dann auch noch darüber, so schadet dies potenziell dem Ruf des Unternehmens. Da solche Angriffe in den letzten zehn Jahren aber häufig geworden sind, nimmt die mediale Aufmerksamkeit inzwischen eher ab (man spricht von einem Gewöhnungseffekt), sodass Unternehmen noch weniger Anreize haben, tatsächlich in Schutzmaßnahmen zu investieren. Leidtragend ist in diesem Fall der Einzelne, dessen persönliche Daten gestohlen wurden.

Das Beispiel verdeutlicht einen wichtigen Grundsatz der Umweltpolitik, nämlich das Verursacherprinzip. Es besagt, dass die volkswirtschaftlichen bzw. sozialen Kosten wirtschaftlicher Aktivitäten oder Unterlassungen von ihrem Verursacher zu tragen sind. Zu diesem Schluss kommen auch Moore und Anderson (Moore und Anderson 2011), die konstatieren: „Systems often fail because the organizations that defend them do not bear the full costs of failure."

Moore und Anderson bemerken weiterhin, dass falsch ausgerichtete Anreize, Informationsasymmetrien und externe Effekte im Bereich der IT-Sicherheit weit verbreitet sind. Das Auftreten von externen Effekten ist aber nicht auf den Bereich der IT-Sicherheit beschränkt, sondern findet sich auch im Bereich des Datenschutzes wieder. Aktuelle Gesetzesänderungen (das deutsche IT-Sicherheitsgesetz, die EU-Datenschutzgrundverordnung) stellen Änderungen in diesem Bereich vor. Es darf jedoch noch bezweifelt werden, ob sie weit genug gehen, um den Großteil des Schadens abzufangen, der nicht bei den Verursachern als Kosten anfällt.

Die fehlenden digitalen Instinkte stellen einen weiteren hochkomplexen Problembereich dar. Sehr verkürzt dargestellt lässt sich vermuten, dass nur ein komplexes Maßnahmenpaket Besserung versprechen kann:

- Auf regulierender Ebene ist eine Pflicht zur Durchführung von Risikoanalysen in wesentlichen Wirtschaftsbereichen, welche auch durch strikte Sanktionen gestärkt wird, vorzusehen.

- Auf technischer Ebene können mittel- bis langfristig Verfahren der Künstlichen Intelligenz die Entscheidungsvorgänge und die Risikobewertung unterstützen, auch wenn deren Entwicklungsschritte schwer vorherzusagen sind. Derzeitige Entwicklungen des Marktes (die gehäufte Akquisition von KI-Firmen durch große Technolo-

gieunternehmen) lassen sich jedoch als Vorzeichen werten, dass bedeutende Fortschritte in diesem Bereich in höherer Frequenz zu erwarten sein werden.[1]

- Auf soziotechnischer Ebene kann etwa in sozialen Netzwerken aggregiertes und zur Verfügung gestelltes Expertenwissen ein Anhaltspunkt für individuelle Risikobewertungen sein.
- Zu begleiten ist dies auch durch verstärkte Anstrengungen im Bildungsbereich. Die Fundamente der digitalen Instinkte sind auch in der Bildung und der Medienkompetenz zu legen. In diesem Bereich lassen sich in der Forschung vermehrt Ansätze der „Gamification" oder „Serious Games" finden, welche eingesetzt werden, um IT-Sicherheits- und Datenschutzkompetenzen an unterschiedlichste Gruppen auf spielerische Weise zu vermitteln.

### *Digitalisierung als Chance für IT-Sicherheit und Datenschutz begreifen*

Neben den Problemfeldern für IT-Sicherheit und Datenschutz, die sich aus der Digitalisierung ergeben, sollen in diesem Abschnitt die Chancen für IT-Sicherheit und Datenschutz dargestellt werden.

In den aufgezeigten Problemfeldern von Datenschutz und IT-Sicherheit lassen sich verschiedene Handlungsfelder für die künftige Wirtschaft, insbesondere die IT-Wirtschaft, ableiten. Die drei Wesentlichen lassen sich konkret benennen:

*I. Sichere und zugleich effiziente Prozesse schaffen*

Im Zuge der Digitalisierung können und müssen etwa in der Arbeitswelt Arbeitsabläufe und Organisationsformen neu überdacht und ausgestaltet werden. Die Nutzung von Schutzmechanismen ist dabei nicht als „Add-on" zu betrachten, sondern im Sinne des „by-Design"-Ansatzes in frühen konzeptionellen Phasen zu beachten. So können nicht nur effiziente, sondern auch zugleich sichere Prozesse geschaffen werden.

*II. Schwachstellen analoger Prozesse beheben*

Schwachstellen in Sicherheitskonzepten finden sich nicht nur in einer durch Digitalisierung im Umbruch begriffenen Welt, sondern auch in traditionellen, analogen Abläufen und organisatorischen Maßnahmen. Durch die Digitalisierung können somit auch bestehende Löcher geschlossen werden, die es bzgl. Informationssicherheit und Datenschutz in vorherigen analogen Prozessen gab.

---

[1] *Kommt es dadurch zu einer zu starken Konzentration bei wenigen Unternehmen, kann dieser Effekt auch ins Gegenteil umschlagen.*

*III. IT-Sicherheit und Datenschutz als Qualitätsmerkmale nutzen*

IT-Sicherheit und hohe Datenschutzstandards können bei geeigneter Positionierung zu Qualitätsmerkmalen werden. Dies betrifft sowohl IKT-Produkte und -Dienste, welche sich somit von Mitanbietern abheben können, als auch z. B. eine innerbetriebliche Ausgestaltung der „digitalisierten" Abläufe. Wird durch die Einführung geeigneter Maßnahmen eine Vertrauenskultur etabliert, so steigert dies auch die Reputation und kann das Anwerben von Fachkräften unterstützen.

### *Fazit*

IT-Sicherheit ist eine Grundbedingung für das Gelingen der Digitalisierung. Die Vertrauenskrise nach Snowden hat dies uns allen unübersehbar bewusst gemacht. In jeder Krise steckt jedoch auch eine Chance: Es könnte sein, dass gerade die Aktivitäten der NSA bewirken werden, dass in Deutschland und Europa eine starke IT-Sicherheitsindustrie entsteht. Die Chancen, die sich im Bereich der IT-Sicherheit und des Datenschutzes für Wirtschaft und Gesellschaft ergeben, sind konsequent zu nutzen.

Neben Gesetzesänderungen/-konkretisierungen oder auch Selbstverpflichtungen der Unternehmen tragen auch niedrigkomplexe, kostengünstige IT-Sicherheitstechnologien zur Sicherheit und zum Schutz der Daten und Persönlichkeitsrechte bei. Eingebettet sind diese jedoch immer in ein größeres System, welches mitbedacht werden muss. Im durch die Digitalisierung ausgelösten Prozess des Neudenkens ist dabei konsequent der „by-Design"-Ansatz zu verfolgen. Das grundlegende Problemfeld der fehlenden digitalen Instinkte erfordert dabei auch nicht zuletzt das Verankern von Kompetenzaufbau auch schon von Beginn an. Instinkte entwickeln sich über längere Zeiträume, etwa seit einem Jahrhundert im Straßenverkehr. Die Geschwindigkeit der Digitalisierung erfordert besondere Anstrengungen.

### *Literatur*

Anderson RJ (2001) Why Information Security is Hard. An Economic Perspective. Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. S 358–365

Bundesministerium des Innern (BMI) (2016) Der Schutz des Rechts auf informationelle Selbstbestimmung. www.bmi.bund.de/DE/Themen/Gesellschaft-Verfassung/Datenschutz/Informationelle-Selbstbestimmung/informationelle-selbstbestimmung_node.html. Zugegriffen: 18.05.2016

Borchers D (2015) Das digitale Ich braucht Verschlüsselung. heise online, 17.10.2015. www.heise.de/newsticker/meldung/Das-digitale-Ich-braucht-Verschluesselung-2849851.html. Zugegriffen: 19.04.2016

Cavoukian A (2011) Privacy by design: the 7 foundational principles. Information and Privacy Commissioner of Ontario. www.ipc.on.ca/images/resources/7foundationalprinciples.pdf. Zugegriffen: 19.04.2016

Cranor LF, Garfinkel S (Hrsg) (2005) Security and usability: designing secure systems that people can use. O'Reilly Media, Sebastopol/Kalifornien

Moore T, Anderson R (2011) Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research. In: Oxford Handbook of the Digital Economy. Oxford University Press, Oxford

Neumann N, Moorfeld R, Reulke K (2016) Die Digitalisierung der Energiewende – vom Smart Grid zur Intelligenten Energieversorgung eingebettet in eine smarte Infrastruktur. In: Wittpahl V (Hrsg) Digitalisierung: Bildung, Technik, Innovation. Institut für Innovation und Technik (iit), Berlin

Weber SG (2014) Alltagstaugliche Biometrie: Entwicklungen, Herausforderungen und Chancen. iit perspektive, Workingpaper Nr. 21. Institut für Innovation und Technik (iit). www.iit-berlin.de/de/publikationen/alltagstaugliche-biometrie-entwicklungen-herausforderungen-und-chancen/at_download/download. Zugegriffen: 19.04.2016

# EFFIZIENZ IN DER DATENAUFBEREITUNG

## Datenvisualisierung zur Kommunikation im politischen Kontext

*Michael Huch, Inessa Seifert*

—

## Datenökonomie und digitale Effizienz – Die Reduktion und Abstraktion von Daten in der vernetzten Welt

*Anett Heinrich, Heiko Kempa, Jochen Kerbusch, Eike-Christian Spitzner*

## 1.2.1 Datenvisualisierung zur Kommunikation im politischen Kontext

*Michael Huch, Inessa Seifert*

*In einer Zeit rasant wachsender Informationen wird deren Nachvollziehbarkeit künftig überhaupt nur durch Aggregation und Verdichtung, etwa durch Text- und Data-Mining-Tools, möglich sein. Zusätzlich bieten sich grafische Visualisierungen an, um ein intuitiveres Verständnis komplexer und mehrdimensionaler Informationen zu ermöglichen. Besonders gelungene Beispiele überlassen es dabei dem Nutzer, sich durch Selektion hinterlegter Daten dynamisch generierte Visualisierungen anzeigen zu lassen, um so den Blick auf spezifische Facetten werfen zu können. Der Beitrag erläutert kurz technische Grundlagen und präsentiert verschiedene Visualisierungsbeispiele, die sich zur Unterstützung politischer Entscheidungen eignen. Am Beispiel der Innovationspolitik werden Anwendungspotenziale für diese neuen Technologien aufgezeigt.*

### *Einführung*

Wir leben in einer Welt, in der immer mehr Informationen generiert und zugänglich gemacht werden. Eine Verarbeitung der weiter stark zunehmenden Informationsmenge wird künftig nur durch Aggregation derselben möglich sein. Ein bekanntes Beispiel für eine händisch aufbereitete Verdichtung von Informationen ist der Wahl-O-Mat der Bundeszentrale für politische Bildung[1], die die Wahlprogramme der zur Wahl stehenden (und an diesem Angebot teilnehmenden) Parteien aufbereitet. Ein politisch interessierter Wähler erhält allein durch die Beantwortung von Fragen, die für den politischen Gestaltungsraum der gewählten Parlamentarier stehen, sein Maß an Übereinstimmung mit einer oder mehreren Parteien angezeigt; er muss sich also nicht mehr durch die Wahlprogramme aller Parteien durcharbeiten, um eine gut informierte Entscheidung für die beste Vertretung der persönlichen politischen Interessen zu fällen.

Auch grafische Visualisierungen kommen zum Einsatz, um – ebenfalls durch Verdichtung – ein intuitiveres Verständnis komplexer und mehrdimensionaler Informationen zu ermöglichen. In den vergangenen Jahren war denn auch eine deutliche Zunahme in der Visualisierung von Informationen zu verzeichnen; insbesondere trifft dies auf Online-Medien zu. Besonders gelungene Beispiele überlassen es dabei dem Nutzer,

[1] *Bundeszentrale für politische Bildung: www.bpb.de/politik/wahlen/wahl-o-mat/. Zugegriffen: 15.03.2016*

sich durch eine Auswahl hinterlegter Daten eine dynamisch generierte Visualisierung anzeigen zu lassen, um so den Blick auf eine spezifische Facette werfen zu können. Im folgenden Beispiel von Spiegel Online können sich Interessierte die Umfrage-

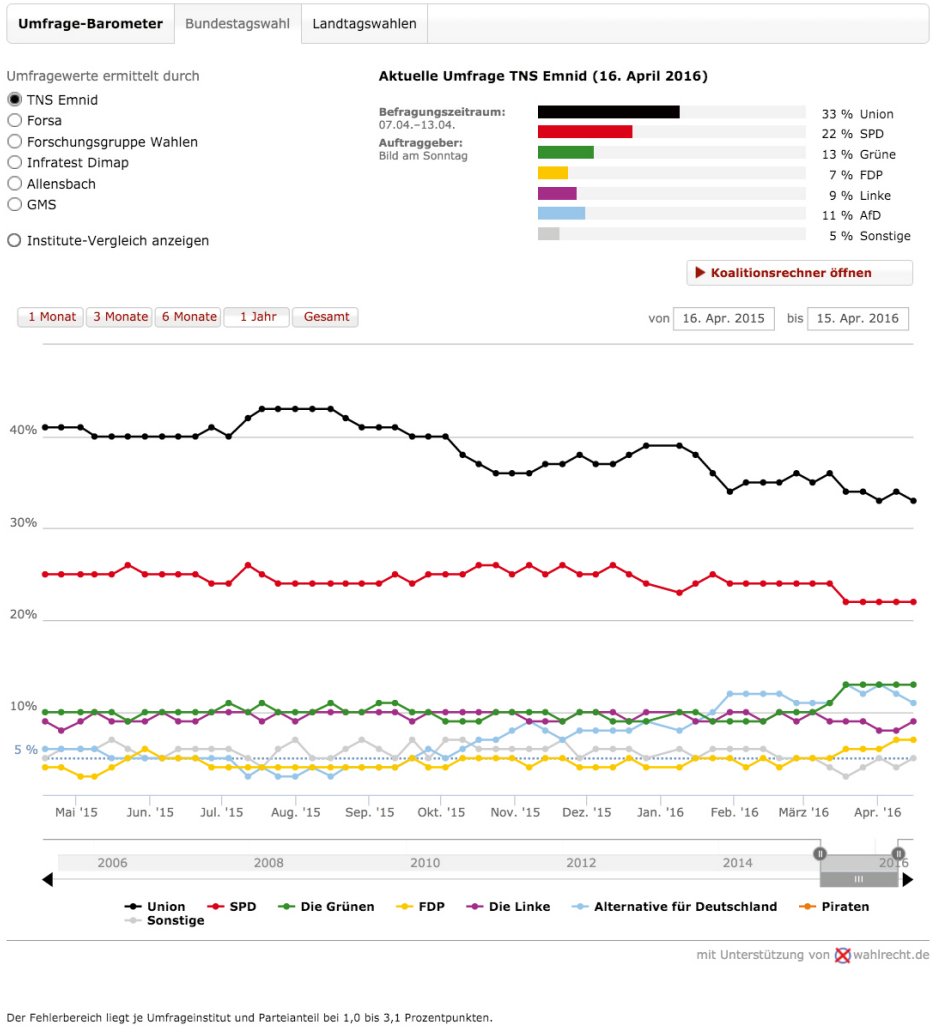


*Abbildung 1.2.1.1: Screenshot der Darstellung von forsa-Umfragen für die Wahlen zum Deutschen Bundestag*[2]

[2] *Spiegel Online: www.spiegel.de/politik/deutschland/sonntagsfrage-umfragen-zu-bundestagswahl-landtagswahl-europawahl-a-944816.html. Zugegriffen: 09.03.2016*

ergebnisse verschiedener Institute zu verschiedenen Wahlen in unterschiedlicher zeitlicher Auflösung anzeigen lassen.

Inwieweit öffentliche Institutionen und Einrichtungen bereits mit Analyse- und Visualisierungstools arbeiten, ist nicht bekannt. Es ist aber zu vermuten, dass deren Verbreitung noch gering ist. Dabei sind die verschiedenen Phasen des Politikzyklus prädestiniert für den Einsatz von Analysewerkzeugen und eine stärkere Visualisierung von Datenbeständen. In allen diesen Phasen, also der Vorbereitung, Durchführung und Nachbearbeitung politischer Maßnahmen, werden vielfältige Informationen genutzt und mindestens in der Durchführung und Nachbereitung eigene Daten generiert.

### *Technische Grundlagen und Visualisierungsbeispiele*

Die Analyse verschiedener bereits öffentlich verfügbarer Datenquellen mit modernen Daten- und Textanalysemethoden birgt viele Potenziale, um neue Erkenntnisse sowohl für die Entscheider aus der Politik und Verwaltung, aber möglicherweise auch für die interessierte Öffentlichkeit zu schaffen.

Der Einsatz von Text- und Data-Mining-Methoden erlaubt bereits heute die automatisierte Analyse von sowohl unstrukturierten als auch strukturierten Daten sowie von Texten. Unstrukturierte Daten liegen normalerweise in einer textuellen oder gemischten Form vor, in der Inhalte gemeinsam mit anderen Informationen enthalten sind. Verfahren zur Informationsextraktion wie Named-Entity-Recognition ermöglichen es, aus unstrukturierten Daten immer wiederkehrende Begriffe (sogenannte Named-Entities) wie Lokationen, Organisationen, Adressen oder Zeitangaben herauszufiltern. Sogenannte Concept-Extraction-Verfahren sind dagegen in der Lage, prominente Begriffe in Dokumenten zu finden bzw. nach speziellen, vom Nutzer vorgegebenen Begriffen zu suchen. Wiederum andere Textverarbeitungsmethoden ermöglichen es, Dokumente über spezifische Relationen zwischen den Konzepten schrittweise zu inspizieren. Text-Mining-Verfahren wie „Clustering" ermöglichen die Zuordnung zahlreicher Dokumente zu thematischen Schwerpunkten. Mit Hilfe der illustrierten Methoden können Nutzer auch ohne spezielle Programmierkenntnisse in unstrukturierte Daten eintauchen und die verborgene Struktur dieser Daten für sich erschließen.

Idealerweise führen im Ergebnis die Analysetools dazu, dass auch vorher unstrukturierte Daten in strukturierter Form vorliegen. Diese Daten können nun von Experten mit den klassischen Methoden der deskriptiven Statistik wie z. B. Berechnungen von Mittelwerten, Standardabweichungen oder auch Erstellung von Regressionsmodellen zur Analyse von Korrelationen zwischen verschiedenen Kerngrößen verarbeitet werden. Die Ergebnisse der Datenanalyse wiederum werden zumeist über programmierbare Import-Schnittstellen (API) an ein Visualisierungstool übermittelt, wo sie in vielfältiger Form kombiniert und visuell dargestellt werden können.

Ein Beispiel für eine ansprechende Datenvisualisierung komplexer Zusammenhänge ist die interaktive Darstellung des Bundeshaushalts. Hier lassen sich sowohl die Einnahmen als auch die Ausgaben, diese zudem nach Ressorts und einzelnen Haushaltstiteln aufgeschlüsselt, anzeigen: Über die Darstellung anhand von Kreissegmenten erhält der Nutzer schnell einen Überblick über Größenordnungen von Einnahmen und Ausgaben.


*Abbildung 1.2.1.2 bis 1.2.1.4: Screenshots der Ausgaben des gesamten Bundeshaushalts (links), des Bundesministeriums für Bildung und Forschung (BMBF) (Mitte) und der BMBF-Ausgaben für „Forschung für Innovationen, Hightech-Strategie" (rechts)*[3]

Von informatorischem Mehrwert für die Öffentlichkeit ist zudem die Möglichkeit dieser Anwendung von Soll-Ist-Vergleichen, die die tatsächlichen Ausgaben unter einzelnen Haushaltstiteln gegenüber dem Plan darstellen. Allerdings fließen in diese konkrete Darstellung keine dynamischen, sondern ausschließlich statische, zu zwei festen Zeitpunkten eines Jahres fixierte, Daten ein: Dies ist zum einen der Bundeshaushalt nach dessen Verabschiedung im Parlament, zum anderen die Haushaltsrechnung des Bundes. Ein wirklich zeitnahes Controlling der Ausgaben gegenüber dem Plan ist hiermit also nicht möglich.

Erste Unternehmen adressieren explizit Regierungsstellen, um diese genau mit dieser Intention, dem zeitnahen Controlling von Ist- gegenüber Soll-Zuständen, durch visuell-unterstützte Analysen bei der Umsetzung öffentlicher Programme zu unterstützen. Die offerierten Lösungen zielen darauf ab, Daten besser zugänglich, verständlich und verwendbar zu machen. Der Vielfalt möglicher Anwendungsbereiche sind kaum Grenzen gesetzt, wie folgendes, stark auf Visualisierungen verschiedener Control-

[3] *Bundesministerium der Finanzen: www.bundeshaushalt-info.de/#/2016/soll/ausgaben/einzelplan/30.html. Zugegriffen: 09.03.2016*

ling-Parameter gestütztes Planungstool zur Koordinierung der Flüchtlingspolitik zeigt.

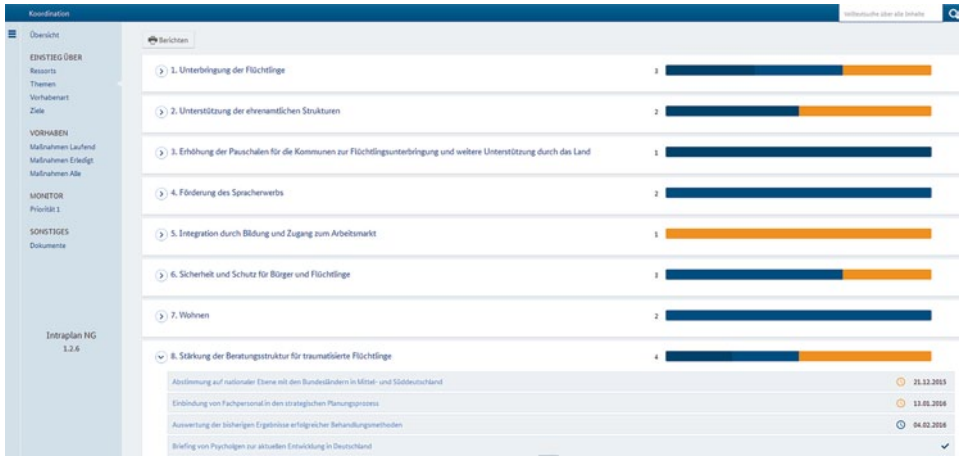


*Abbildung 1.2.1.5: Screenshot eines Planungstools zur Koordination der Flüchtlingspolitik*[4]

Bei dieser Lösung werden einzelne Aspekte der Koordinierung über verschiedene grafische Visualisierungen hinsichtlich ihres Umsetzungsstandes angezeigt. Wichtig ist, dass solche Lösungen vor Beginn der Durchführung von politischen Maßnahmen einsetzen, um einerseits klar festzulegen, welche Daten(quellen) genutzt werden und andererseits sinnvolle Kriterien für die Bewertung des Umsetzungsfortschritts festzulegen.

Andere Anbieter aus dem Bereich Business-Analytics stellen bereits jetzt zahlreiche Lösungen zur Verfügung, die sowohl die Analyse von strukturierten als auch von unstrukturierten Daten ermöglichen. Laut einer Studie (Parenteau et al. 2016) geht der aktuelle Trend in Richtung sogenannter „self-service"-Lösungen. Nutzer dieser Business-Analytics-Software erhalten die Möglichkeit, ohne Unterstützung eines IT-Dienstleisters, d. h. selbstständig, verschiedene Datenquellen in ein Analyse-System einzubinden, dabei Data- und Textanalyseverfahren auszuwählen und miteinander zu kombinieren. Zum Schluss stellen solche Business-Analytics-Lösungen eine Reihe von Visualisierungstools zur Verfügung, mit denen die Ergebnisse der Analyse mittels Balkendiagrammen, geografischen Karten oder zahlreichen anderen Darstellungen visualisiert und veröffentlicht werden können.

[4] *Agendo – Gesellschaft für politische Planung: www.agendo.de/content/intraplan-flow. Zugegriffen: 09.03.2016*

### *Internationale Visualisierungsbeispiele für die Innovationspolitik*

Im Folgenden richtet sich der Blick spezifischer auf Anwendungspotenziale in der Innovationspolitik. Ein erstes Beispiel für vielfältige und interaktive Datenvisualisierungen ist die P3-Datenbank (Projects, People, Publications) des Schweizerischen Nationalfonds (SNF). Aktuell werden der interessierten Öffentlichkeit sechs visuelle Einstiegsmöglichkeiten zum Informationsabruf angeboten, etwa über eine Landkarte der Schweiz, auf der die geförderten Hochschulen dargestellt sind; einer Weltkarte, die Länder nach Anzahl der Kooperationen in verschiedenen Farbtiefen darstellt; oder eine Präsentation nach verschiedenen Wissenschaftsdisziplinen. Der Nutzer dieses Angebotes kann durch individuelle Klicks weitere Informationsebenen aufrufen. Letztlich liegt allen visualisierten Ergebnissen eine vielfältig mit sich selbst verknüpfte Datenbank für Projekte, Personen und Publikationen zu Grunde, die bis in das Jahr 2005 zurückgeht.

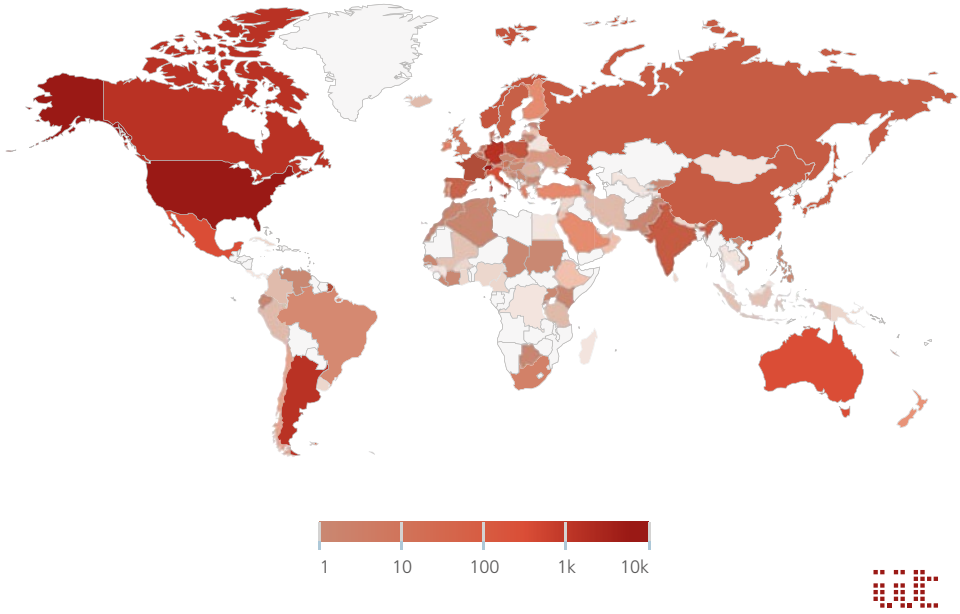


*Abbildung 1.2.1.6: Interaktive Weltkarte zur Darstellung der Kooperationsintensität Schweizer Forscher*[5]

[5] *Schweizerischer Nationalfonds zur Förderung der wissenschaftlichen Forschung (SNF): p3.snf.ch/Default.aspx?id=intcollab. Zugegriffen: 18.03.2016*

Eine noch etwas weitergehende Präsentation innovationspolitischer Fördermaßnahmen ist das für die Öffentlichkeit konzipierte interaktive Dashboard (Instrumententafel) des Natural Sciences and Engineering Research Council of Canada (NSERC). Über das Dashboard werden dem Nutzer Visualisierungen mehrerer Datenquellen angezeigt, die zwei- bis dreimal jährlich aktualisiert werden – etwa in Form einer Landkarte, die Fördermittel je Region darstellt oder Nachrichten zu spezifischen Forschungsthemen präsentiert. Viele der dargestellten Informationen enthalten wiederum Hyperlinks, die dann z. B. zu einzelnen geförderten Vorhaben führen.

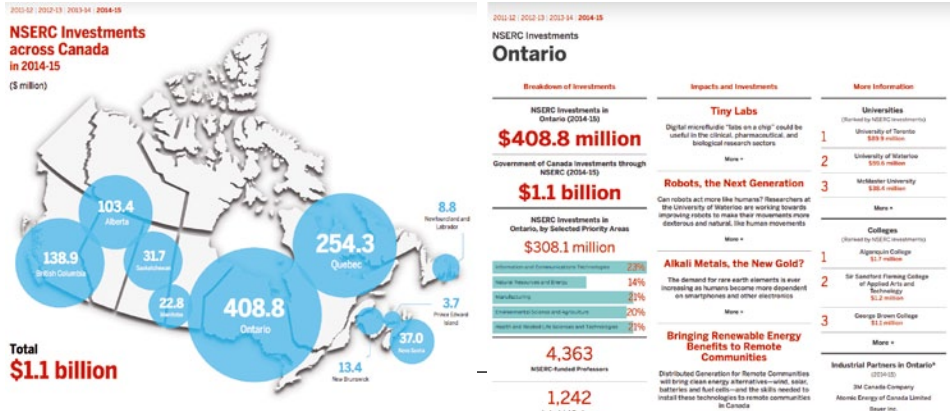


*Abbildung 1.2.1.7 und 1.2.1.8: Screenshots des NSERC-Dashboards*[6]

Über die Darstellung der Eingangsseite – oben links abgebildet – kann sich der Nutzer die öffentlichen Investitionen für die einzelnen Provinzen Kanadas bereits für unterschiedliche Haushaltsjahre anzeigen lassen. Ein Klick auf einen der Kreise – für das Beispiel Ontario oben auf der rechten Seite abgebildet – stellt neue Informationen dar, etwa die prozentuale Verteilung auf Förderthemen oder eine Rankingliste der Universitäten und Colleges, die die meisten Fördermittel zugesprochen bekamen. Zusätzlich sind im mittleren Bereich der Webseite inhaltlich passende Nachrichten dargestellt, die spezifisch einzelne Ergebnisse („Wirkungen") der Investitionen präsentieren. Dieses Beispiel zeigt das Potenzial auf, innovationspolitisches Regierungshandeln hoch aggregiert einer interessierten Öffentlichkeit auf transparente Weise näher zu bringen.

[6] *Natural Sciences and Engineering Research Council of Canada (NSERC): www.nserc-crsng.gc.ca/db-tb/index-eng.asp. Zugegriffen: 01.03.2016*

### *Status und Potenziale der Datenvisualisierung für die deutsche Innovationspolitik*

In Deutschland ist der „Förderkatalog der Bundesregierung“[7] die öffentlich zugängliche Datenbank zur Recherche von geförderten Forschungsvorhaben. Sie beinhaltet aktuell mehr als 15.500 Vorhaben für das Bundesministerium für Bildung und Forschung (BMBF) und mehr als 4.600 für das Bundesministerium für Wirtschaft und Energie (BMWi). Die Ergebnisse werden in rein tabellarischer Form ausgegeben; sie umfassen eine beschränkte Auswahl an Parametern, etwa Name und Ort des Zuwendungsempfängers, die Fördersumme und die Laufzeit des Vorhabens und darüber hinaus administrative Informationen zur Leistungsplansystematik, zum zuständigen Referat im BMBF und zum Projektträger.

Visualisierungen sind nicht Teil dieses Angebotes. Aber bereits die durch den Förderkatalog bereitgestellten Informationen bieten Ansätze für sinnvolle und leicht zu realisierende Visualisierungen. So könnte unter Nutzung der Adressen und der vom BMBF bewilligten Fördermittel eine grafische Landkarte schnell verdeutlichen, in welchen Regionen Deutschlands sich Forschungseinrichtungen und Unternehmen häufen, die erfolgreich bei der Einwerbung von öffentlichen Forschungsmitteln sind. Diese Information könnte wiederum mit Clusterlandkarten abgeglichen werden, um zu prüfen, wie weit die Schwerpunkte regionaler Fördermittelverteilung mit den identifizierten Clustern übereinstimmen.

Die „Clusterplattform Deutschland“ unterhält auch bereits eine landkartengestützte Präsentation von mehr als 100 Clustern, bei denen ein Nutzer nach verschiedenen Parametern (Technologiefeld, Bundesland, nach Art der Förderung oder Auszeichnung eines Clusters) filtern kann.

Die Nutzerfreundlichkeit dieses Informationsangebotes schließt neben der dynamischen Landkartendarstellung – beispielsweise führt ein Klick auf einen Kreis mit mehreren Treffern zu einer feiner aufgelösten Kartengröße – auch die Anzeige der Ergebnisse in Tabellenform mit ein. Dort hinterlegte Hyperlinks führen zu den Webseiten der angezeigten Organisationen. Die zugrundeliegenden Informationen sind jedoch zu einem spezifischen Zeitpunkt fixiert worden, basieren also nicht auf dynamischen Datenquellen.

Bis jetzt nicht öffentlich zugänglich in Deutschland, aber in der Regel bereits vorhanden und mit großem Potenzial für Analysen und grafische Aufbereitungen, sind weitere Informationen zum Inhalt eines geförderten Vorhabens, sei es in Form von fest-

[7] *Die Bundesregierung: foerderportal.bund.de/foekat/jsp/StartAction.do. Zugegriffen: 01.03.2016*


*Abbildung 1.2.1.9: Screenshot der Ergebnisse für deutsche Clusterorganisationen*[8]

gelegten deskriptiven Meta-Daten zum Forschungsgebiet oder in Form einer textlich gefassten Kurzbeschreibung des Vorhabens. Über die Analyse der Inhalte geförderter Vorhaben könnten Relationen zwischen verwendeten Technologien und ihren Anwendungsbereichen identifiziert werden. So zeigt beispielsweise der Abgleich über die Begriffe „angewandt" oder „findet Verwendung" den Zusammenhang von Technologien und Anwendungen auf. Über weitere Bearbeitungsschritte wären dann auch Darstellungen von regionalen Schwerpunkten für Forschung zu bestimmten Technologien und ihren Anwendungen möglich. Dies wiederum könnte für eine Verifizierung dahingehend genutzt werden, ob bereits identifizierte Cluster auch wirklich mit regionalen Förderschwerpunkten übereinstimmen.

Würden nun weitere Datenquellen berücksichtigt, etwa Patentdatenbanken, bibliometrische Verzeichnisse, wissenschaftsbezogene Artikel aus Fachjournalen

[8] *Bundesministerium für Wirtschaft und Energie: www.clusterplattform.de/CLUSTER/Navigation/Karte/SiteGlobals/Forms/Formulare/karte-formular.html. Zugegriffen: 29.03.2016*

*Abbildung 1.2.1.10: Screenshot einer Patentlandkarte*[9]

und der Presse oder auch spezifische Diskussionsforen aus sozialen Medien, und setzt man oben genannte Analyseverfahren und Visualisierungen ein, können neue Erkenntnisse für die Innovationspolitik gewonnen werden. Im folgenden Beispiel kombiniert ein Unternehmen Informationen aus Patentdatenbanken mit den Ortsangaben der jeweiligen Erfinder und stellt einander ähnliche Patentklassen grafisch für einen begrenzten regionalen Raum – im Beispiel für Berlin – in Form einer „neuen Landkarte" dar. Eine Häufung von inhaltlich naheliegenden Patenten wird dann – ähnlich auch bei „heat maps" – optisch betont, im Beispiel als geografische Erhebung. Thematisch weit auseinanderliegende Patente, die auf ganz anderen Technologien beruhen, werden als durch „Wasserflächen" getrennte Landflächen angezeigt.

Mit Hilfe dieser neuen Tools könnten auch Forschungs-Outputs, in der Regel Ergebnisse einer Forschungsarbeit, oft in Form von Publikationen oder Patentanmeldungen, in eine Analyse geförderter Vorhaben einbezogen werden. Damit lässt sich zumindest ex-post die Effektivität – d. h. die Input- (öffentlicher Mitteleinsatz)/Output- (Ergebnisse der geförderten Vorhaben) Relation – der staatlichen Zuwendungen in den Blick nehmen.

[9] *mapegy: www.mapegy.com/de/news/technologieradar-berlin. Zugegriffen: 29.03.2016*

### *Ausblick*

Neue Analysetools und fortschreitende Speicher- und Datenverarbeitungskapazitäten erschließen immer weitere Datenquellen, die in neuen Kombinationsformen zu neuen Erkenntnissen führen können. Gegenüber einer rein textlichen und/oder numerischen Präsentation von Inhalten verschaffen Visualisierungen oft bereits durch einen anderen, intuitiveren Zugang neue Einsichten. Dabei sind die Einsatzzwecke für Datenvisualisierungen äußerst vielfältig, wie die vielen Beispiele in diesem kurzen Text verdeutlichen.

In hoch-aggregierter Form könnten die in diesem Beitrag dargestellten Analysen und Visualisierungen perspektivisch die Prioritätensetzung z. B. der deutschen Innovationspolitik mit der Hightech-Strategie[10] begleiten, indem sie einerseits die zugrundeliegenden Annahmen für diese Schwerpunkte analytisch-visuell unterstützen und andererseits fortlaufend die Entwicklung der ausgewählten Schwerpunkte in der Umsetzungsphase begleiten und die gesetzten Prioritäten validieren oder alternative Tendenzen aufzeigen.

Regierungsstellen in Deutschland sind jedoch noch zurückhaltend im Einsatz dieser neuen Technologien. Dabei böte eine auf mehreren Datenquellen basierende dynamische und nutzerspezifische Visualisierung großes Potenzial. Dies gilt insbesondere für ein fortlaufendes Controlling der Umsetzung politischer Maßnahmen. Die fortlaufende Einspeisung neuer Informationen zum Umsetzungsfortschritt verschafft über Datenvisualisierungen einen transparenten und stets aktuellen Überblick über die laufenden bzw. abgeschlossenen Prozesse.

Ebenso könnte die Transparenz des Regierungshandelns noch gesteigert werden, indem öffentlich zugängliche Informationsangebote nutzerspezifische Aggregationsmöglichkeiten auf auswählbare Informationen anbieten, wie die zuvor präsentierten Beispiele aus der Schweiz und aus Kanada zeigen.

### *Literatur*

Parenteau J, Sallam RL, Howson C, Tapadinhas J, Schlegel K, Oestreich TW (2016) Magic Quadrant for Business Intelligence and Analytics Platforms. Gartner, Inc. www.gartner.com/doc/reprints?id=1-2XXET8P&ct=160204&st=sb. Zugegriffen: 19.04.2016

[10] *Prioritäre Zukunftsaufgaben für Wertschöpfung und Lebensqualität. Die Bundesregierung: www.hightech-strategie.de/de/Prioritaere-Zukunftsaufgaben-82.php. Zugegriffen: 10.03.2016*

## 1.2.2 Datenökonomie und digitale Effizienz – Die Reduktion und Abstraktion von Daten in der vernetzten Welt

*Anett Heinrich, Heiko Kempa, Jochen Kerbusch, Eike-Christian Spitzner*

*Die Digitalisierung erfordert die Bereitstellung enormer Datenmengen. Diese werden mit Hilfe von vernetzten Sensoren gewonnen. Neben der Quantität ist vor allem die Qualität dieser Daten entscheidend für darauf basierende, innovative Anwendungen. Ein oft unterschätzter, aber wesentlicher Beitrag hierzu ist eine leistungsfähige und effiziente Datenvorverarbeitung. Statt riesige Mengen unbearbeiteter Rohdaten von lokalen Sensoren an Steuerrechner bzw. Big-Data-Infrastrukturen zu schicken, ist es oft sinnvoller, bereits am Ort der Messung auf wesentliche Informationen zu reduzieren. Darüber hinaus bietet dieser hardwarebasierte Ansatz ein erheblich höheres Maß an Datensicherheit und -schutz, da nur das Minimum an erforderlichen Informationen übertragen und zentral gespeichert wird.*

### *Motivation und Vision*

In immer mehr Bereichen des täglichen Lebens hält die Digitalisierung Einzug, um uns den Alltag zu erleichtern. Schlagworte wie Internet der Dinge, Industrie 4.0, Smart Home oder Telemedizin sind in aller Munde. Der Schlüssel zur Innovation in diesem Feld liegt in der Vernetzung intelligenter Geräte und der damit möglichen Nutzung vieler, dezentral gewonnener Daten. Die Vision ist das umfassende Sammeln aller verfügbaren Informationen, um sie auszuwerten und auf dieser Basis verschiedenste Dienstleistungen anzubieten. Dabei ist neben der Quantität vor allem die Qualität der genutzten Daten entscheidend für die Qualität der darauf basierenden Anwendungen. Ein wesentlicher Beitrag hierzu ist eine leistungsfähige und effiziente Datenvorverarbeitung. Statt riesige Mengen an Informationen von lokalen Sensoren an eine übergeordnete Infrastruktur zu schicken, ist es oft sinnvoller, den Datenstrom mit Hilfe effizienter Hardware bereits am Ort der Messung auf die für die Verarbeitung wesentlichen Informationen unter Berücksichtigung von Datensicherheit und Datenschutz zu reduzieren.

### *Ein typischer Tag in der digitalisierten Welt*

Der Wecker klingelt. Dank der Sensorik, die den Schlaf überwacht hat, nicht in einer Tiefschlafphase. Im Bad erkennt die Zahnbürste zu viel Druck und weist den Nutzer

darauf hin, dass er bestimmte Zähne vernachlässigt. Die Kaffeemaschine kennt den individuellen Kaffeekonsum. Auch der Herd schaltet sich automatisch ab, wenn das Wasser zum Kochen der Eier überläuft. Beim Frühsport erkennt der Fitnesstracker den Puls und die Schrittzahl, der smarte Schuh weist auf einen schlechten Laufstil hin. Die intelligente Waschmaschine misst automatisch Beladung sowie Verschmutzung und sorgt für die richtige Dosierung des Waschmittels. Zum Auto: Durch die Speicherung der gewünschten Sitz-, Spiegel- und Lenkradposition auf dem Smartphone werden die personifizierten Einstellungen direkt beim Einstieg ins Auto vorgenommen. Auf dem Weg zur Arbeit überwachen Radar-, Ultraschall- sowie optische Sensoren die Fahrt. GPS-gemessen kennt das Fahrzeug stets seine Position. Mit all diesen Systemen weist es auf den Radfahrer hin, den man beim Abbiegen fast übersehen hätte. Auch das Rad verfügt über Sensoren und GPS, die das Licht nur bei Dunkelheit einschalten und den Weg weisen. Der Fahrer trägt statt eines Helmes einen Airbag, der sich bei einem Unfall sensorgesteuert ausgelöst hätte. In der Tiefgarage am Arbeitsplatz überwachen Sensoren die Belegung, LEDs zeigen den Weg zum nächsten freien Platz. Der Mitarbeiterausweis wird an jeder Tür erkannt und gewährt Zutritt. In den Produktionshallen überwachen Sensoren den Gefahrenbereich, um Kollisionen mit unbemannten Fahrzeugen oder Montagerobotern zu vermeiden. Kontinuierlich wird per Umweltkontrolle die Luft auf Giftstoffe untersucht. Maschinen lassen sich aus der Ferne bedienen und melden Fehlfunktionen oder das nahende Ende eines Wartungszyklus. Feierabend. Sensoren registrieren die Einkäufe und beschleunigen das Kassieren. Der Einkaufswagen merkt, wenn er das Gelände des Marktes verlässt und schlägt Alarm. Zurück zu Hause lauscht der Fernseher auf Sprachbefehle und erkennt, ob sich jemand vor dem Gerät befindet und richtet es entsprechend aus.

So könnte ein ganz normaler Tag in einer Welt voller Sensoren aussehen. Die Darstellung ist sicher unvollständig, aber alle Beispiele sind bereits Realität, wobei typische Vertreter wie die zahllosen Überwachungskameras, Bewegungsmelder, Verkehrsüberwachungsanlagen, Temperaturfühler, Windmesser etc. noch gar nicht berücksichtigt wurden. Auch die umfassende Vernetzung der einzelnen Sensoren und die Verschmelzung der Daten in der Cloud wurden hier noch nicht betrachtet.

### *Was bedeutet „vernetzte Welt“?*

Im Beispiel handelt es sich zumeist um Sensor- und Elektroniksysteme, die jeweils auf Basis relativ weniger Messdaten vereinzelt auch online kommunizieren, aber lokal begrenzt agieren. In Summe sind die gewonnenen Informationen jedoch vielfältig und ermöglichen zusammengeführt noch deutlich höherwertige Dienstleistungen. Doch was bedeutet es technisch, wenn wirklich alle Sensoren alle Messdaten permanent über Datennetze an eine oder mehrere externe Stellen senden?

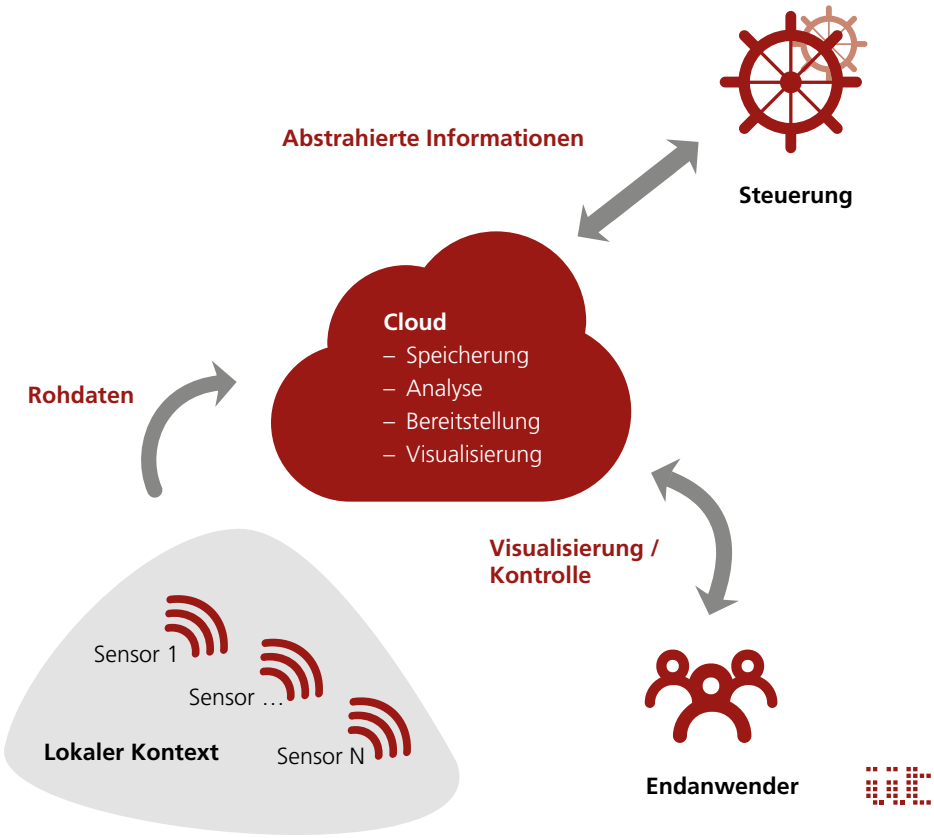


*Abbildung 1.2.2.1: Übliches Konzept der Cloud-basierten Dienste: Lokale Sensoren kommunizieren alle Rohdaten zur Auswertung und Bereitstellung an die Cloud, auf die Endanwender sowie Steuerungsinstanzen zugreifen können.*

Heute greifen etwa 15 Milliarden Geräte auf das Internet zu. Durch das Internet der Dinge wird diese Zahl zweifelsfrei stark anwachsen. Manche Experten gehen von bis zu 50 Milliarden weltweit vernetzten Geräten im Jahr 2020 aus (Hein 2015), andere von 500 Milliarden im Jahr 2030 (BMWi 2015). Smarte Systeme[1] sind in der Regel dauerhaft in Betrieb. Dauerhaft große Datenmengen durch das Internet zu senden, ist

[1] *Smarte Systeme sind eigenständige intelligente, technische Komponenten mit erweiterter Funktionalität, die in der Lage sind, ihre Umgebung zu erfassen, einen Zustand zu analysieren, darauf aufbauend Vorhersagen und Entscheidungen zu treffen und auf ihre Umwelt Einfluss zu nehmen. Sie sind hoch-miniaturisiert, vernetzt und meist energieunabhängig.*

jedoch schon aus technischer Sicht keine Lösung: Geht man von 500 Milliarden Geräten aus, so würde bereits das Verschicken je eines einzelnen IP-Datenpaketes (kleinste Einheit im Internet-Übertragungsprotokoll) pro Sekunde enorme Übertragungskapazitäten voraussetzen, vergleichbar mit Hunderten von Millionen Nutzern, die gleichzeitig ultrahochaufgelöstes Fernsehen über das Internet empfangen. Und dies ist eine Minimalbetrachtung. Sendet eine größere Menge von vernetzten Sensorsystemen unverarbeitete Rohdaten, so wird der Ansatz, alle Daten ohne Vorverarbeitung zu senden, allein aus Gründen der Übertragungskapazitäten technisch unmöglich.

### *Was bedeutet „Reduktion und Abstraktion von Daten“?*

Um die wachsende, aus wirtschaftlichen Gründen aber immer begrenzte Bandbreite nicht zu sprengen, sind Konzepte erforderlich, die die Datenflut eindämmen. Dies kann durch Auslassen von Messwerten geschehen. Nicht für alle Anwendungen sind Echtzeitdaten erforderlich, sondern weitaus längere Messintervalle ausreichend. Doch das ist nur ein Anfang. Ein Sensor, der periodisch einen Messwert zur Zustandsüberwachung ausgibt, produziert und kommuniziert Unmengen an irrelevanten Daten über den Normzustand. Stattdessen kann ein regelmäßiges Lebenszeichen und gegebenenfalls ein Fehlersignal gesendet werden. Erst im Fehlerfall sind weitere Informationen erforderlich, die bedarfsgerecht abgerufen werden können. Neben einer Reduktion der zu übertragenden Datenmenge ermöglicht eine Vorverarbeitung durch effiziente Hardware auch ein erhöhtes Maß an Schutz der Privatsphäre. Wer möchte z. B., dass der Fernseher permanent die Umgebung auf Sprachbefehle hin überwacht, indem er einen permanenten Datenstrom an einen zentralen Server der Herstellerfirma zur Auswertung sendet?

Abgesehen von sehr einfachen Ausnahmen ist für die maschinelle Auswertung und Interpretation von Sensordaten ohnehin eine Vorverarbeitung erforderlich. Von Sensorsystemen erzeugte Daten müssen in der Regel für die Verarbeitung durch komplexere Software konditioniert werden. Dafür existieren zahlreiche mathematische und informationstechnische Verfahren, die auf den jeweiligen Anwendungsfall zugeschnitten zum Einsatz kommen und der Bereinigung, Reduktion und Extraktion von Daten dienen.

Die zugrundeliegenden Algorithmen können sowohl als Software als auch als Hardware in Form von diskreten oder integrierten mikroelektronischen Schaltungen umgesetzt werden. Bei herkömmlichen Anwendungen wird die Datenvorverarbeitung in derselben Hardwareumgebung wie die eigentliche Datenauswertung ausgeführt und typischerweise als Software implementiert. Dadurch werden Hardwarekosten eingespart und Flexibilität bei der Programmierung gewonnen. Auf der anderen Seite müssen alle Rohdaten übermittelt werden, was die Bandbreite belastet, Sicherheitsfragen aufwirft und ein hohes Maß an Energie kostet.

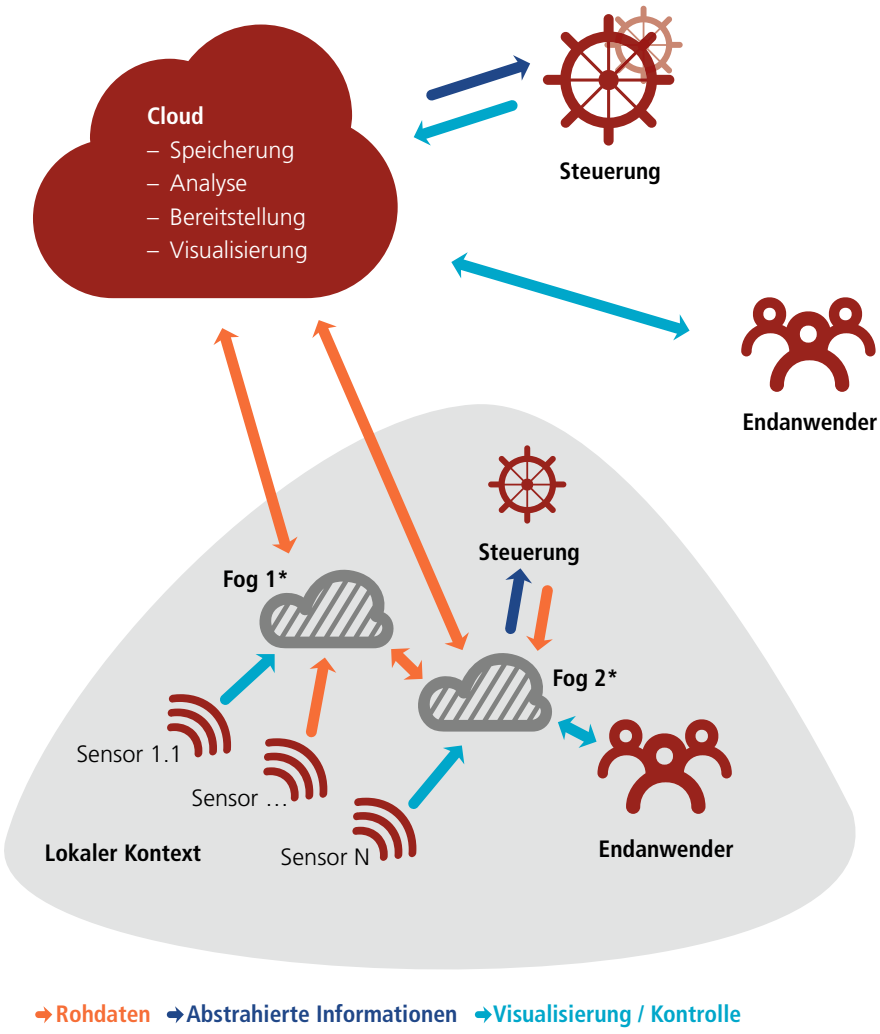


*Abbildung 1.2.2.2: Konzept der abstrahierten Kommunikation: Lokale Sensoren kommunizieren abstrahierte und/oder Rohdaten an einen lokalen Verbund („Fog"), der wiederum nur abstrahierte Daten an die Cloud weiterleitet oder von dort erhält bzw. den Zugriff im lokalen Kontext erlaubt. Über die Cloud können externe Endanwender sowie Steuerinstanzen nur indirekt auf die Sensordaten zugreifen.*

Um ausreichende Sicherheitskonzepte zu etablieren, müssen Unternehmen zunächst investieren. Ein Lösungsansatz besteht in einer effektiven und effizienten, hardwarebasierten Datenvorverarbeitung auf Sensorebene oder hierarchisch gestaffelt auch auf Ebene eines oder mehrerer Gateways, die die Daten aus vielen Sensoren zu einer Gesamtinformation verschmelzen und abstrahieren, wie es mit dem „Fog Computing" vorgeschlagen wurde.[2] Dies muss bereits vor der Vernetzung geschehen, da nachträgliche Versuche meist zum Scheitern verurteilt sind. Wichtige Aspekte, die für die Sicherheit in Betracht gezogen werden sollten, sind einerseits die Weiterleitung und Speicherung von lediglich notwendigen Daten, eine Verschlüsselung der zu übertragenden Daten sowie ein separater Schutz der gespeicherten Daten am Sammelpunkt (Server). Angriffe auf die Sicherheit lassen sich grundsätzlich nicht ausschalten. Daher gilt es den Angreifern so wenig Angriffsfläche wie möglich zu bieten. Vorteil der hardwarebasierten Datenvorverarbeitung direkt am Sensor ist die selektive Weitergabe von Informationen. Nur hardwarebasiert kann ein definitives Aussortieren von Daten realisiert werden. Dies führt zu einer Reduktion der zu übertragenden Daten. Daten, die gar nicht erst an Softwarekomponenten übergeben oder übertragen werden, müssen nicht geschützt werden.

### *Worin bestehen die Herausforderungen?*

Die Anforderungen an Systeme zur Datenvorverarbeitung sind stark widersprüchlich: Einer der wichtigsten Aspekte ist die Echtzeitfähigkeit der Datenreduktion, die nur durch eine hohe Rechenleistung erzielt werden kann. Diese wiederum erfordert entweder einen hohen Energieeinsatz (Mikrocontroller) oder eine starke Spezialisierung auf Hardwareebene (sog. ASICs). Ersteres führt wiederum zu verkürzten (Akku-)Laufzeiten, Letzteres zu einem Verlust an Flexibilität und erhöhten Kosten. Der Entwicklungsaufwand für ASICs ist vor allem bei kleinen Stückzahlen sehr hoch. Weiterhin können an eine spezielle Aufgabe angepasste Verarbeitungssysteme nicht auf einfache Weise während der Lebensdauer an neue Bedürfnisse angepasst werden. Ihre Funktionen und ihre Datenausgabe werden zum Zeitpunkt der Entwicklung vorgegeben, eine in der Hardware nicht vorgesehene Funktion kann kaum nachträglich hinzugefügt werden. Modifikationen sind nur in geringem Umfang möglich. Dem gegenüber steht eine erheblich höhere Leistungsfähigkeit der spezialisierten Funktionen bei gleichzeitig geringerem Energieverbrauch als bei softwarebasierten Systemen, die auf Mikrocontrollern ausgeführt werden. Gerade im Bereich der Sensornetzwerke ist dies ein sehr wichtiger Aspekt, da einzelnen batteriegespeisten Knoten nur geringe Energiemengen zur Verfügung stehen.

[2] *FOGnetworks: fognetworks.org/whitepapers. Zugegriffen: 18.05.2016*

Es muss also ein Kompromiss aus Leistungsfähigkeit, Energieeffizienz und Flexibilität gefunden werden. Dieser kann jedoch nicht allgemeingültig formuliert werden, da das Anwendungsspektrum zu breit ist, sondern muss anwendungsspezifisch aufgestellt werden. Dabei würde ein modularer Baukasten – aus Hardwarekomponenten für spezifische, besonders zeit- und energiekritische Aufgaben sowie Softwaremodulen für den flexiblen Einsatz – maßgeschneiderte Lösungen ermöglichen.

Aus Sicht der Systemanbieter müssen Systeme zur Datenreduktion und Abstraktion neben der Möglichkeit des Maßschneiderns anwendungsspezifischer Lösungen einfach in der Handhabung und Integration sein. Dies kann nur durch ein hohes Maß an Selbstorganisation und Selbstkonfiguration erreicht werden. Jedoch bergen solche automatisierten Routinen sicherheitsrelevante Risiken in sich.

Aus Sicht der Endanwender stehen vor allem die großen wirtschaftlichen Chancen im Vordergrund, die durch eine allumfassende Vernetzung und darauf basierenden Geschäftsmodellen entstehen. Wichtig ist dennoch, dass die Datenflut idealerweise schon am Ort der Messung gefiltert wird, denn Daten an sich schaffen keinen Wettbewerbsvorteil, sondern dieser hängt von der Auswertung ab.

Beispielsweise kann die Vernetzung von Geräten und Prozessen im Gesundheitswesen die Effizienz von Behandlungen und Pflege steigern. So lassen sich Gesundheitsdaten von Patienten unabhängig vom Aufenthaltsort automatisiert erfassen und auswerten. Diese Vernetzung birgt neben enormen wirtschaftlichen Chancen für Unternehmen auch erhebliche Risiken des Informationsmissbrauchs – noch deutlicher als im Beispiel des lauschenden Fernsehers. Das Zusammenführen von Daten ohne eine demokratische Legitimation und Kontrolle birgt inhärent das Potenzial einer informationellen Ausbeutung und kann die Grundrechte der Menschen massiv verletzen. Der Zugriff auf persönliche Daten und deren Monetarisierung durch Weitergabe an Dritte kann zudem zu einer nicht unerheblichen Änderung der Geschäftsbeziehung führen. Vergütet der Nutzer eine Dienstleistung mit seinen Daten und nicht mit Geld, so ist er nicht mehr der Kunde, sondern im Prinzip die Ware. Zudem kann die Datenweitergabe unerwünschte Folgen haben, z. B. bei Bewerbungsverfahren im Berufsleben oder bei Versicherungen. Deshalb spielen umfassende Sicherheitskonzepte in der vernetzten Welt eine zentrale Rolle. Alle Systeme, die über das Internet miteinander verbunden sind, können kompromittiert und die darin übermittelten Daten missbraucht werden. Es gilt der Grundsatz: „Alles was gehackt werden kann, wird auch gehackt!" (Sabine Herlitschka, Vorstandsvorsitzende Infineon Austria, in Dobrowolski 2015). Somit ist jedes mit dem Internet verbundene Gerät grundsätzlich in Gefahr.

Umfassendes Risikomanagement ist also ein weiterer wichtiger Aspekt für erfolgreiche Systeme zur Datenreduktion und Abstraktion, der hauptsächlich in den in der ISO 27001 abgebildeten Bereichen Datenverfügbarkeit, Datenintegrität sowie Datensicherheit im Sinne von Zugangskontrolle und Datenverlust wiedergegeben wird. Ein

hoher Grad an Verschlüsselung sowie der inhärent erhöhte Schutz der Privatsphäre durch die Abstraktion von Daten am frühestmöglichen Punkt im System bilden dafür die Grundlage. Verfügbarkeit und Integrität sind für das einwandfreie Funktionieren in der Cloud angesiedelter Anwendungen erforderlich. Hier muss im Einzelfall abgewogen werden, wie kritisch die Verfügbarkeit der auf den Daten basierenden Anwendung ist. Im gleichen Zuge bestehen hohe Anforderungen an die Datenqualität. Die Abstraktion wird per se die Qualität erhöhen, jedoch müssen die anwendungsspezifischen Systeme eine entsprechend hohe Erkennungsrate aufweisen. Insbesondere bei der Überwachung kritischer Funktionen dürfen wichtige Ereignisse nicht „übersehen" werden. Fehlalarme sind zwar ebenfalls unerwünscht, wären aber durch eine Überprüfung als solche erkennbar und deshalb als weitaus weniger kritisch einzustufen.

***Fazit***

Der Bedarf an einer effizienten Datenvorverarbeitung, d. h. einer Reduktion und Abstraktion von Daten, ist evident. Weiterhin sind auf den individuellen Anwendungsfall maßgeschneiderte Lösungen unerlässlich. In vielen Fällen ist dabei ein hardwarebasierter Ansatz aufgrund der besseren Sicherheit sowie der höheren Effizienz einer reinen Softwarelösung vorzuziehen. Die technischen Voraussetzungen dafür sind im Wesentlichen bereits heute erfüllt. Die größten Hürden bestehen im Fehlen einer Standardisierung, einem Mangel an modularen, kompatiblen Konzepten und in der Tatsache, dass eine Standardtechnologie ausgewählt werden müsste, auf der anschließend immer weiter aufgebaut wird, anstatt immer neue Technologien aufzusetzen. Darüber hinaus ist der Ansatz, den Idealzustand in der Verschmelzung und Analyse aller theoretisch verfügbaren Informationen zu sehen, kritisch zu hinterfragen.

Erst mit Einzug der genannten Faktoren in die Umsetzung von vernetzten, digitalen Dienstleistungen kann eine für alle Seiten vorteilhafte Wertschöpfung erfolgen. Für kleine und mittelständische Unternehmen sind hardwarebasierte Lösungen, die speziell auf ihre Anwendungsgebiete ausgerichtet, zugleich stromsparend und angriffsgeschützt sind, eine nicht unerhebliche Investition. Um auch diese Unternehmen von hardwarebasierten Lösungen zur Datenvorverarbeitung überzeugen zu können, ist es notwendig, standardisierte Einzelpakete dieser Hardware als einen individuell erweiterbaren Baukasten zu entwickeln und diese dann in der Massenproduktion kostengünstig anzubieten. Erst damit können neue Geschäftsmodelle aufgebaut und bestehende der Zeit angepasst werden. Die Anbieter solcher Systeme profitieren von einem Standard durch neue Produkte. Nicht zuletzt profitieren die Anwender von einfacher, sicherer Handhabung und von der Gewissheit, dass ein Informationsmissbrauch erschwert wird. Datensicherheit kann, ebenso wie Energieeffizienz und Benutzerfreundlichkeit, in einer Welt im Wandel niemals ein Zustand sein, sondern wird immer ein Prozess bleiben.

### *Literatur*

Bundesministerium für Wirtschaft und Energie (BMWi) (2015) Impulse für die Digitalisierung der deutschen Wirtschaft. Digitale Agenda des BMWi. www.bmwi.de/BMWi/Redaktion/PDF/I/impulse-fuer-die-digitalisierung-der-deutschen-wirtschaft. Zugegriffen: 19.04.2016

Dobrowolski P (2015) „Pflegeroboter sind eine attraktive Idee". Wiener Zeitung, 12.12.2015. www.wienerzeitung.at/themen_channel/wz_reflexionen/zeitgenossen/790661_Pflegeroboter-sind-eine-attraktive-Idee.html. Zugegriffen: 19.04.2016

Hein M (2015) Kommentar: Internet der Dinge. Risiken des IoT. funkschau, 05.03.2015. www.funkschau.de/datacenter/artikel/117680. Zugegriffen: 19.04.2016