Mensch und Technik in Interaktion

Wie gelingt individuelle digitale Souveränität?

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Digital
Autonomy Hub
Technik souverän nutzen

Grußwort

UNSER ALLTAG, OB PRIVAT ODER BERUFLICH, wird immer digitaler. Egal, ob bei Online-Bestellungen, Videokonferenzen oder zuhause im Smart Home: In vielen Lebensbereichen nutzen wir digitale Technologien. Dabei hinterlassen wir zahlreiche Daten im Netz. Aber wissen wir auch immer, wem wir unsere Daten geben? Oder wozu sie genutzt werden? Persönliche Daten weiterzugeben, ist nicht grundsätzlich falsch, das zeigt etwa die Corona-Warn-App. Aber oft sind wir uns gar nicht bewusst, was mit unseren Daten im Netz passiert. Oder wir sind aufgrund des Aufwands und der Komplexität entmutigt herauszufinden, wie wir bei der Datenweitergabe mitreden können.

Deshalb hat das Bundesministerium für Bildung und Forschung (BMBF) die Fördermaßnahme „Mensch-Technik-Interaktion für digitale Souveränität (DISO)“ ins Leben gerufen. So fördert es Projekte, die Menschen dabei helfen, selbstbestimmt und reflektiert mit ihren Daten und digitalen Technologien umzugehen. Kurz gesagt: Ihre digitale Souveränität zu stärken.

Digitale Souveränität ist ein Querschnittsthema, das viele Technologien und unterschiedliche Themen berührt. Genauso vielfältig und unterschiedlich sind auch die Themen der Projekte, die das BMBF mit DISO fördert. Zum Beispiel wird eine Augmented-Reality-Anwendung für ein Smart Home entwickelt, die Datenströme visualisiert. Sie sehen mit eigenen Augen, welche Geräte im Smart Home welche Daten sammeln. Oder es entsteht ein digitaler Assistent, der Jugendlichen durch verschiedene Micro-Games spielerisch Datenschutz-Kompetenzen beibringt. In die Entwicklung des Assistenten wurden Jugendliche miteinbezogen.

Das ist wichtig, denn: Bei allen Innovationen muss der Mensch im Mittelpunkt stehen. Die Technikentwicklung muss potentielle Nutzerinnen und Nutzer von Anfang an mit an Bord holen. Es gilt herauszufinden, wie sie ermutigt werden können, sich mit der Datenverwendung in digitalen Technologien auseinanderzusetzen und wie diese für sie verständlich gemacht werden kann. Die geförderten Projekte sind interdisziplinär und berücksichtigen technologische genauso wie juristische, ethische und sozialwissenschaftliche Erkenntnisse. Nur so findet eine Technik den Weg in unseren Alltag, die verantwortungsvoll mit unseren Daten umgeht und mit der wir souverän umgehen können.

Diese Publikation präsentiert Ihnen die ganze Bandbreite unserer Forschungsprojekte zu digitaler Souveränität. Ich wünsche Ihnen eine spannende und informative Lektüre!

Prof. Dr. Veronika von Messling
Leiterin Abteilung „Lebenswissenschaften“
Bundesministerium für Bildung und Forschung

Mensch und Technik in Interaktion
WIE GELINGT INDIVIDUELLE DIGITALE SOUVERÄNITÄT?
DIGITAL AUTONOMY HUB

Impressumsangaben:
November 2021

Veröffentlicht von
Gesellschaft für Informatik e. V.
Geschäftsstelle Berlin
Spreepalais am Dom – Anna-Louisa-Karsch-Str. 2 – 10178 Berlin

AW AlgorithmWatch gGmbh
Linienstr. 13 – 10178 Berlin

Kontakt
Info@digitalautonomy.net
Webseite
www.digitalautonomy.net

Redaktion (Gesellschaft für Informatik e. V.)
Paula Böhme
Cin Pietschmann
Elisabeth Schauermann
Inga Sell
Umfrage Ipsos GmbH
Korrektorat Carlos Gluschak
Gestaltung Daniela Greven
Illustration Julia Praschma

Gefördert durch das Bundesministerium für Bildung und Forschung

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
Digital Autonomy Hub
Technik souverän nutzen
GESELLSCHAFT FÜR INFORMATIK
ALGORITHM WATCH

Inhalt

Vorwort

Über 70 % der Menschen in Deutschland sind besorgt um ihre Daten bei der Nutzung digitaler Dienste und über 90 % bemühen sich zumindest hin und wieder um Datenschutz in der alltäglichen Nutzung von Diensten und Geräten – Datenmündigkeit in der Techniknutzung ist ein relevantes und herausforderndes Thema.

Das Kompetenzzentrum „Digital Autonomy Hub – Technik souverän nutzen“ verfolgt das Ziel, allen Menschen einen reflektierten und selbstbestimmten Umgang mit Technologie zu ermöglichen. Die vom Bundesministerium für Bildung und Forschung (BMBF) im Forschungsprogramm „Miteinander durch Innovation“ geförderten Projekte, die wir seit 2020 in ihrer angewandten Forschung begleiten, entwickeln innovative nutzerzentrierte Lösungen, um Menschen mehr Wissen und bessere Handhabe über ihr digitales Leben und ihre persönlichen Daten zu geben.

Vor diesem Hintergrund führten wir im Frühjahr 2021 mit dem Forschungsinstitut Ipsos eine repräsentative Umfrage durch, in der wir Menschen nach ihren persönlichen Einstellungen, Sorgen und Hoffnungen in der alltäglichen Techniknutzung befragten. In dieser Publikation präsentieren wir die Ergebnisse und ordnen sie mithilfe von Expert·innen ein. Mit Perspektiven aus Informatik, Pädagogik, Ethik, Recht und Wirtschaftswissenschaften tragen wir der Breite unserer Fragestellungen in dieser Publikation Rechnung.

Stimmen aus dem Beirat des Digital Autonomy Hubs reflektieren unseren transdisziplinären Ansatz bereits in der Gesamtschau und machen hoffentlich Lust auf einen tieferen Einstieg in die Lektüre. Im Kapitel „Privatheit und Datenschutz“ gehen wir auf Sorgen und Risiken für die Privatsphäre, aber auch auf individuelle und gesellschaftliche Möglichkeiten für einen mündigen Umgang mit Daten ein. Daran anschließend beleuchten wir im Kapitel „Digitale Kompetenzen“ die unterschiedlichen Bedarfe und Möglichkeiten für den Kompetenzaufbau und den souveränen Umgang mit Technologie in jedem Alter. Schließlich stellen wir im Kapitel „Technologieentwicklung“ Erfolgsfaktoren für eine Steigerung der individuellen digitalen Souveränität vor und zeigen innovative Ideen für Mensch-Technik-Interaktionen. Im Format „Innovative Einblicke“ stellen wir die zehn Forschungsvorhaben des Digital Autonomy Hubs vor, die im Programm „Mensch-Technik-Interaktion für digitale Souveränität“ gefördert werden.

Wir hoffen, Ihnen mit der vorliegenden Publikation einen Einstieg in den Themenkomplex rund um individuelle digitale Souveränität in der Techniknutzung zu bieten und Möglichkeiten für Innovationen aufzuzeigen. Das Team des Digital Autonomy Hubs wünscht Ihnen viel Freude und spannende Einsichten beim Lesen.

Elisabeth Schauermann
Projektleiterin Digital Autonomy Hub
Gesellschaft für Informatik e. V.

Methoden-steckbrief

METHODIK

Das Marktforschungsunternehmen Ipsos wurde beauftragt, mit quantitativen Methoden den Status quo im Hinblick auf Techniknutzung, digitale Kompetenzen, Datenschutzwissen und -maßnahmen sowie Informationsverhalten in der deutschen Bevölkerung zu erforschen. Ebenso Teil dieser Studie war die Erforschung passender Lösungsansätze, die zur digitalen Ermächtigung beitragen können.

STUDIENTEILNEHMENDE

Deutschsprachige Allgemeinbevölkerung ab 18 Jahre

ERHEBUNGSMETHODE

Computer Assisted Web Interviews (CAWI)

STICHPROBE UND GEWICHTUNG

Proband·innen wurden durch das Ipsos Online Access Panel geworben. Die Stichprobe wurde nach Alter, Geschlecht, Region und Bildungsstand quotiert und nach Alter, Geschlecht und Region gewichtet.

BEFRAGUNGSZEITRAUM UND ANZAHL DER BEFRAGTEN

Die Befragung wurde im März 2021 durchgeführt. Für die finale Auswertung wurden die Daten von insgesamt 2000 Fragebögen verwendet.

EINORDUNG

Durch die Verwendung von CAWI schließt die Stichprobe ausschließlich Proband·innen ein, die Zugang zu einem Computer mit Internetverbindung haben und über ein Grundverständnis der Computernutzung verfügen.
Die qualitativen Beiträge von Expert·innen dienen der Einordnung der Umfrageergebnisse und erlauben eine Betrachtung von Fragestellungen und Zusammenhängen, die in einer quantitativen Umfrage nicht abgebildet werden können.

1/ GESAMTSCHAU: SECHS PERSPEKTIVEN AUF DIGITALE SOUVERÄNITÄT

Das Digital Autonomy Hub wird von Vertreter·innen der Netzwerkprojekte sowie von externen Expert·innen beraten. Der Beirat begleitet die Aktivitäten des Hubs, um den Themenkomplex „individuelle digitale Souveränität“ für Politik, Wirtschaft, Zivilgesellschaft und Wissenschaft fundiert aufzubereiten. Um die verschiedenen Perspektiven der digitalen Souveränität zu beleuchten, setzt sich der Beirat transdisziplinär zusammen. Sechs Stimmen der Mitglieder haben wir aufgegriffen. Sie gehen darauf ein, welche Aspekte aus rechtlicher, gesellschaftlicher, technischer, ökonomischer, ethischer und medienpädagogischer Perspektive relevant sind.

RECHT

„Echte Selbstbestimmung basiert auf individueller digitaler Souveränität: Menschen sollen in der Regel selbst über den Umgang mit ihren Daten bestimmen können – ganz ohne Beeinflussung, Druck oder das Gefühl der Ohnmacht angesichts der Komplexität von IT-Systemen. Aus Bequemlichkeit nehmen viele Fremdbestimmung in Kauf und ohne ausreichendes Verständnis und Risikobewusstsein sind Missbrauch und Manipulation Tür und Tor geöffnet. Daher müssen die rechtlichen Vorgaben der Datenschutz-Grundverordnung ernst genommen werden. Insbesondere muss ‚Datenschutz by Default‘ der Startpunkt einer jeder Verarbeitung personenbezogener Daten sein.“

Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein, ULD

GESELLSCHAFT

„Während Konsument·innen in der freien Marktwirtschaft die Wahl haben, wo welche persönlichen Daten weitergegeben werden – bspw. kann man zwischen etlichen E-Commerce-Anbietern oder Messenger-Anwendungen auswählen oder auch auf deren Angebote ganz verzichten –, besteht diese Wahlfreiheit im öffentlichen Sektor nicht. Um Leistungen in Anspruch nehmen zu können oder um rechtliche Anforderungen zu erfüllen, müssen Bürger·innen entsprechende Dienste nutzen und teilweise hochsensible Daten bereitstellen. Diese besondere Beziehung zwischen dem Staat und den Bürger·innen erfordert es, dass Maßnahmen zur Erhöhung der digitalen Souveränität besonders sorgfältig gestaltet werden."

Prof. Dr. Moreen Heine, E-Government und Open Data Ecosystems, Universität zu Lübeck

TECHNIK

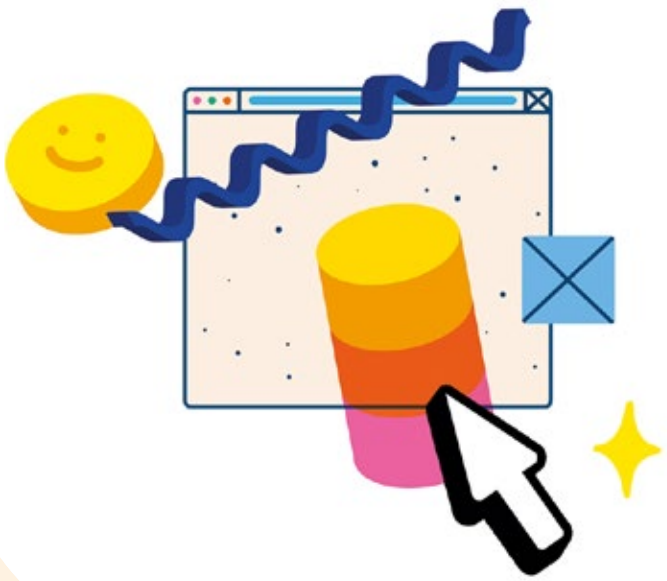
„In der Softwareentwicklung ist es wichtig, vertrauenswürdige Software gemeinsam mit den Nutzenden zu entwickeln und Assistenzmechanismen für alle Typen von Nutzer·innen einzubauen. Ich vertraue einem System mehr, wenn die Software bereits automatisiert offenlegt, welche ihre internen Mechanismen sind und wie z. B. persönliche Daten verarbeitet oder Entscheidungen getroffen werden. Intelligente Assistenz bietet den jeweiligen Nutzer·innen an sie und deren Kontext angepasste Hilfestellungen. Durch die Nutzung von modellbasierten und generativen Entwicklungsmethoden kann man solche Mechanismen bereits automatisiert integrieren und erleichtert es so weniger technikaffinen Menschen, selbstbestimmt Systeme zu nutzen."

Dr. Judith Michael, Lehrstuhl für Software Engineering, RWTH Aachen

WIRTSCHAFT

„Digitale Geschäftsmodelle nutzen Daten als Schlüsselressource für die Wertschöpfung. Heute ‚bezahlen' Nutzer·innen daher häufig mit ihren Daten, ohne genau zu verstehen, was damit passiert oder was diese wert sind. Hier fehlt häufig noch die Transparenz seitens der Unternehmen. Damit sich das ändert, sind bei der Entwicklung digitaler Geschäftsmodelle auch die Perspektiven von Ökonomie, Informatik, Ethik und Recht einzubeziehen. Unsere Forschung zeigt, dass dieser interdisziplinäre Ansatz Unternehmen dabei unterstützt, wirtschaftlich tragfähig zu agieren und die Souveränität von Nutzer·innen zu stärken."

Dr. Marija Radić, Fraunhofer IMW



MEDIENPÄDAGOGIK

„Elektronische Datenverarbeitung verändert seit Jahrzehnten die Grundlagen unseres Zusammenlebens, Maschinenlernen hat diese Veränderungen beschleunigt. Solche technologischen Bedingungen unserer Gesellschaft zu reflektieren und zu verstehen, muss ein zentrales Ziel von Bildungsarbeit sein. Nur wenn Menschen in die Lage versetzt werden, sich diese Fragen zu erschließen, sie zu bewerten und echte Handlungsoptionen zu entwickeln, können wir demokratische Teilhabe stärken, um auch mit neuen Technologien eine gerechte und solidarische Gesellschaft zu schaffen."

Robert Behrendt, medialepfade

ETHIK

„Ethik sucht und prüft kraft praktischer Vernunft Kriterien und Ermöglichungsbedingungen ‚guten Lebens'. Sie liefert eine Checkliste, nach der man die digitale Wirtschaft und Gesellschaft verantwortlich ausgestalten kann:

- Welche Gestaltungsoption wird allen am meisten nützen und am wenigsten schaden? (utilitaristischer Ansatz)
- Welche Option respektiert die Rechte aller Beteiligten am besten? (Rechte-Ansatz)
- Welche Option wird Menschen gleich oder doch fair behandeln? (Gerechtigkeitsansatz)
- Welche Option eignet sich am besten für die gesamte Gesellschaft? (Gemeinwohlansatz)
- Welche Option ermöglicht mir, als die Art von Person aufzutreten, die ich sein möchte? (Tugendethik-Ansatz)"

Prof. Dr. Wolfgang M. Schröder, Universität Würzburg

2/ PRIVATHEIT UND DATENSCHUTZ

Sorgen um die eigene Privatsphäre sind in einer zunehmend digitalisierten Welt verbreitet, eng verbunden hiermit sind Fragen zum Schutz der persönlichen Daten. Auf individueller und gesellschaftlicher Ebene bestehen sowohl Möglichkeiten für den Datenschutz als auch Hürden in der Umsetzung. In diesem Kapitel wird ein Blick auf Datenschutz und Privatheit im Spannungsfeld von Theorie und Praxis geworfen.

Privatheit und damit verbundene Sorgen *Interview mit Prof. Dr. Sabine Trepte*

Zunächst eine grundlegende Frage: Was ist Privatheit überhaupt?

Prof. Dr. Sabine Trepte: Sie steigen mit der schwierigsten Frage ein! Ich gebe mein Bestes: Also, mir gefällt die Idee von Privatheit als bedürfnisorientierte Zugänglichkeit. Privatheit fühlen Menschen je nachdem, wie zugänglich sie für andere sind und ob diese Zugänglichkeit ihren Bedürfnissen in einer bestimmten Situation entspricht. Wenn Sie also beispielsweise U-Bahn fahren, niemand etwas von Ihnen erfahren soll und Sie diesen Wunsch auch umsetzen können, dann entspricht die Situation Ihren Vorstellungen von Zugänglichkeit. Und wenn Sie beispielsweise mit drei Freund·innen in Ihrer Küche sitzen und plaudern und gern viel von sich berichten möchten, dann entspricht dies ebenfalls Ihren Vorstellungen von Zugänglichkeit. Beide Situationen entsprechen einem Empfinden von Privatheit, obwohl Sie anderen Menschen in der einen Situation sehr wenig, in der anderen sehr viel preisgeben.

Wie hängt nun Privatheit mit Datenmündigkeit in der Techniknutzung zusammen?

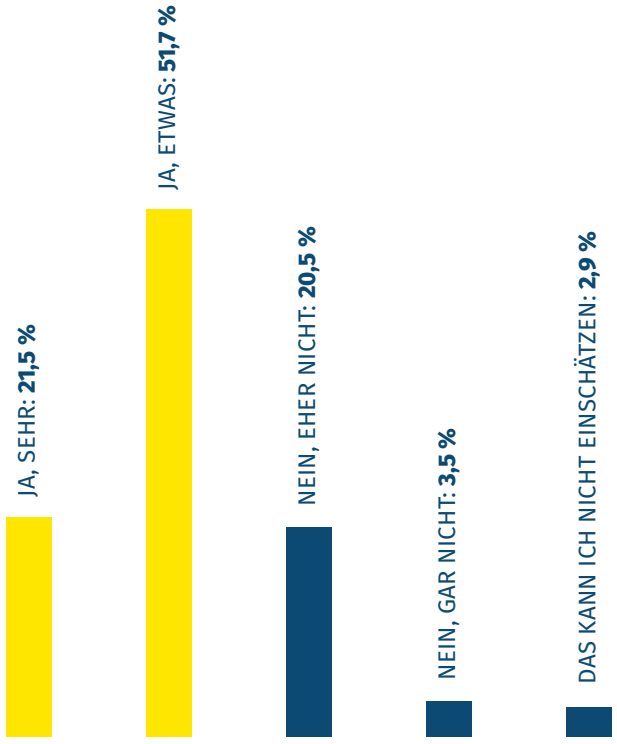
Informationelle Selbstbestimmung oder Datenmündigkeit implizieren genau den Kern der gerade genannten Idee von Privatheit. Bei der informationellen Selbstbestimmung geht es nämlich nicht nur darum, wie viel oder was Menschen von sich preisgeben, sondern ob dies ihren Bedürfnissen entspricht und ob es in einer bestimmten Situation angemessen ist. Und hier fällt schon etwas auf:

Die Beurteilung, ob die Verwendung von Daten den Bedürfnissen eines Menschen entspricht oder angemessen ist, setzt voraus, dass sie überhaupt wissen, dass Ihre Daten erhoben werden und was damit gemacht wird. Das ist heute bei den meisten Anwendungen nicht der Fall. Manchmal ist das ein echter Jammer, denn es wäre gut, wenn die Menschen besser informiert wären und informierte Entscheidungen über die Datenverwendung treffen könnten. Manchmal ist es aber auch gar nicht erforderlich. An manchen Stellen helfen soziale und regulative Normen weiter und schützen Menschen. Normen regeln, dass beispielsweise Internetnutzende sich nicht in alles hineindenken müssen. In diese Normen vertrauen zu können, ist genauso wichtig wie die selbstbestimmte Entscheidung.

In unserer repräsentativen Studie geben rund 70 % der Befragten an, dass sie besorgt darüber sind, dass digitale Geräte und Anwendungen Daten über sie sammeln und verarbeiten. Nur wenige machen sich jedoch große Sorgen. Deckt sich dieser Befund mit Ihren Erfahrungen?

Ja, die meisten Studien über die Sorgen zur Privatheit zeigen, dass die Mehrheit der Deutschen nach wie vor um die Verwendung der eigenen Daten besorgt ist. Das sind zu viele, die sich Sorgen machen! Wenn Menschen Sorgen haben, dann deutet dies darauf hin, dass ihnen Informationen fehlen, dass ihre Kontrollbedürfnisse noch nicht ausreichend ernst genommen oder wahrgenommen werden. Die Sorgen der Menschen sind gleichzeitig für uns ein wichtiger Hinweis: Wir haben noch viel zu tun damit, für die informationelle Selbstbestimmung zu kämpfen. Zum Glück sind Wissenschaftler·innen, Datenschützer·innen, Jurist·innen und viele andere Expert·innen nach wie vor sehr aktiv dabei, das zu verbessern. Eigentlich sollten wir das Internet nutzen können, ohne uns große Sorgen im Allgemeinen zu machen. Aber bitte sorgen Sie sich weiter, wenn es um spezifische Anwendungen geht. Zum Beispiel, wenn Sie sich bei einem neuen Portal anmelden, bitte machen Sie sich Sorgen! Das führt nämlich dann dazu, dass Sie sich informieren, die Meinung anderer einholen und nachdenken.

Die Mehrheit der Befragten (73,2 %) ist besorgt, dass digitale Geräte und Anwendungen Daten über sie sammeln.



Basis: alle Befragten (n = 2000). Darstellung der Top 2 und Bottom 2. Angaben in Prozent. Frage Q5: Sind sie besorgt darüber, dass digitale Geräte und Anwendungen (z. B. Apps, Webseiten, Smartphones) Daten über Sie sammeln und verarbeiten?

Wie gehen Menschen mit Privatheit um? Wie können wir verstehen, dass einige Menschen gerne und freiwillig ihre Laufzeiten oder Fotos online teilen, sich aber dennoch Sorgen über ihre Datenspuren machen?

Sorgen sind ein Gefühl der Unsicherheit, der Zurückhaltung, bei stärkeren Sorgen können sie in Angst münden. Sorgen sind aus psychologischer Perspektive ein wichtiger Indikator für uns Menschen, dass wir mehr Informationen benötigen, dass wir nicht Ruhe geben können, dass wir uns mit anderen austauschen möchten. Sorgen sind ein Ausrufezeichen auf unserer To-Do-Liste. Bedeutet dieses Ausrufezeichen, dass wir

alle damit assoziierten Aktivitäten einstellen? Auf keinen Fall! Sorge bedeutet erst einmal, dass wir wachsam sein müssen und nicht unbedingt, dass wir das Verhalten einstellen.

Hat sich der Umgang mit Privatheit durch die verstärkte Techniknutzung in den vergangenen zehn, zwanzig Jahren gewandelt?

Das Bedürfnis nach Privatheit, Privatheitssorgen und auch der Wert der Privatheit ändern sich nicht über die Zeit bzw. die Veränderungen sind marginal. Der Umgang mit Privatheit bei der Nutzung einzelner Dienste – beispielsweise ob Menschen ihren Klarnamen angeben, ob und wie sie die Datenschutzeinstellungen ändern oder umgehen – hat sich jedoch verändert. Die meisten sind gut informiert und nutzen drei Formen des Datenschutzes: Erstens werden die Datenschutzeinstellungen in den Diensten selbst aktiv angepasst. Zweitens sind immer mehr Menschen anonym über den Onion-Browser im Internet unterwegs, um keine Spuren der Online-Recherche zu hinterlassen und so die kommerzielle Verwendung der eigenen Verhaltensdaten zu vermeiden. Drittens verschleiern Menschen gern Aspekte ihrer Identität, nutzen also keine Klarnamen, wenn sie im Internet unterwegs sind.

Die Besorgnis um die eigene Daten ist unabhängig von der Nutzungshäufigkeit digitaler Anwendungen und Produkte.

Basis: alle Befragten (n = 2000). Darstellung der Top 2 und Bottom 2. Angaben in Prozent. Frage Q5: Sind sie besorgt darüber, dass digitale Geräte und Anwendungen (z. B. Apps, Webseiten, Smartphones) Daten über Sie sammeln und verarbeiten?
© Ipsos | Digital Autonomy Hub

Prof. Dr. Sabine Trepte, Universität Hohenheim
© privat

Sabine Trepte ist Professorin für Kommunikationswissenschaft, insbesondere Medienpsychologie an der Universität Hohenheim in Stuttgart. Ihre Forschungsschwerpunkte liegen im Bereich Privatheit und soziale Medien. Besonders interessiert sie die psychologische Perspektive auf den Wandel der Privatheit und wie Medien diesen Wandel beeinflussen.

Datenschutz stört meine Arbeit *Beitrag von M1$c*

Welche Daten geben wir von uns preis? Und wer interessiert sich überhaupt für unsere Daten? Oft sind die Opfer von Cyberangriffen keine berühmten Persönlichkeiten, sondern arglose Personen, deren Daten besonders einfach zugänglich sind.

Hallo, ich bin M1$c und bezeichne mich selbst als Data-Hunter. Ich beschaffe, verarbeite, und verkaufe persönliche Daten. Bei meinen Aufträgen bin ich nicht wählerisch: Hauptsache, es bringt Geld ein.

Einer der einfachsten Jobs ist es, ein Profil über eine Person anzulegen. Viele Online-Dienste ermöglichen es mir, gebündelt an alle öffentlich verfügbaren Informationen über eine Person zu kommen. Praktischerweise haben die Leute bei fast allen sozialen Medien ein Profilbild. So sehe ich gleich, dass ich die richtige Person gefunden habe. Xing und LinkedIn verraten mir dann nicht nur, wo die Leute schon überall gearbeitet haben, sondern auch den aktuellen Wohnort. Mit ein bisschen Social-Engineering bekomme ich fast immer auch die Adresse heraus. Dafür reicht ein Anruf bei der aktuellen Arbeitsstelle; ich gebe mich als Sekretär·in der vorherigen Firma aus und sage, wir hätten noch Unterlagen, die wir nachschicken müssen. Solange man sehr nett ist und unbeholfen tut, bekommt man, was man will. Die Leute freuen sich oft sogar, mir zu helfen.

Sich dumm stellen, funktioniert meist auch sehr gut, um die Zwei-Faktor-Authentifizierung zu umgehen: „Ich kann mich nicht mehr einloggen … ich weiß nicht, welchen Knopf ich da drücken muss." Das zur Umgehung benötigte Geburtsdatum geben viele bereitwillig online an, etwa wenn sie stolz ein Bild ihres Geburtstagskuchens twittern. Manchmal muss ich nicht einmal anrufen, um die notwendigen Informationen zu bekommen. Die Smartphones, die wir mit uns herumtragen, speichern in jedem Bild den Standort, an dem es aufgenommen wurde. So erfahre ich nicht nur, wo die Person wohnt, sondern auch, wo sie am liebsten essen geht, wo sie jeden Morgen auf dem Weg zur Arbeit vorbeikommt, und dass sie gerade im Urlaub ist. Die vielen Bilder mit der Katze zeigen mir außerdem, dass diese Person allein wohnt und welche Wertgegenstände in der Wohnung stehen. Oder ganz generell, was für Interessen die Person hat.

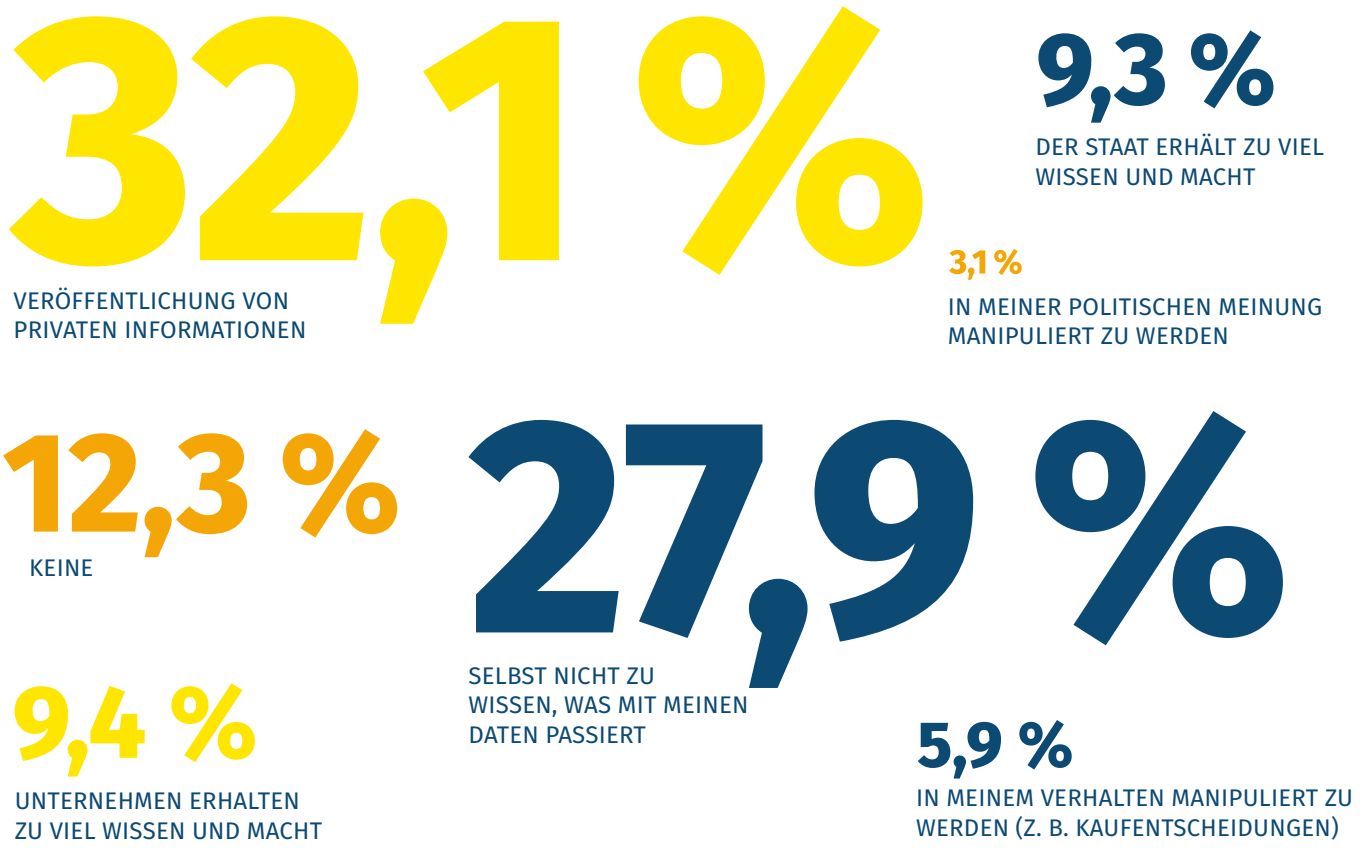
87,7 % der Befragten befürchten negative Folgen durch die Speicherung, Verarbeitung und Nutzung ihrer persönlichen Daten durch digitale Technologien.[I]

Das sind alles sehr einfache Möglichkeiten – ich selbst habe nur ein paar Tage gebraucht, um sie mir beizubringen. Dass der Aufwand dafür gering ist, merkt man auch an den vielen Angriffen, die täglich stattfinden. Spear-Phishing ist eine weitere einfache Möglichkeit, an Daten zu kommen. Mit sehr einfachen HTML-Programmier-Skills baut man eine bekannte Webseite nach. Muss nicht perfekt sein, muss meine Opfer ja nur dazu bewegen, ihre Daten in mein Formular einzugeben. E-Mail, Passwort, Sicherheitsabfrage, vielleicht noch die IBAN – und schon kann es losgehen. Auch Gewinnspiel-Formulare eignen sich super, um schnell an viele E-Mail-Adressen zu kommen. Allein die Chance auf den Gewinn reicht, damit die Leute ihre Daten hergeben. Ein halbes Jahr später verschicke ich dann Spam. Das ist zu viel Zeit, als dass sie noch nachvollziehen können, was die eigentliche Ursache für den Spam war.

Eine Telefonnummer ist übrigens fabelhalft. Fast alle Dienste erwarten heutzutage, dass man eine angibt. So

I Basis: alle Befragten (n = 2000). Darstellung derer, die mindestens eine negative Folge auswählten. Frage Q7: Welche negativen Folgen befürchten Sie durch die Speicherung, Verarbeitung und Nutzung Ihrer persönlichen Daten durch digitale Technologien? Bitte klicken Sie die Items nach empfundener Negativität geordnet an. 1 = am negativsten, 2 = am zweitnegativsten, etc..© Ipsos | Digital Autonomy Hub

Am meisten fürchten sich die Befragten vor der Veröffentlichung von privaten Informationen.



Basis: Befragte, die negative Folgen sehen (n = 1755). Darstellung des Rang 1. Frage Q7: Welche negativen Folgen befürchten Sie durch die Speicherung, Verarbeitung und Nutzung Ihrer persönlichen Daten durch digitale Technologien? Bitte klicken Sie die Items nach empfundener Negativität geordnet an. 1 = am negativsten, 2 = am zweitnegativsten etc..© Ipsos | Digital Autonomy Hub

kann ich auch andere Accounts finden und weiß, dass sie zur selben Person gehören. Die Nummer ist ja fast so eindeutig wie die Personalausweisnummer.
Am meisten Spaß an meinem Job macht mir allerdings die Manipulation von Menschen. Wenn man es richtig macht, verstehen sie nicht einmal, dass sie manipuliert wurden. Absurd, aber die meisten Menschen fühlen sich gefeit vor politischer Manipulation. Schon klar, niemand will beeinflussbar sein. Aber war es wirklich eine ganz eigene autonome Idee, nicht wählen zu gehen, um damit „ein Zeichen zu setzen“? Oder habe ich die politische Meinung herausgefunden, sie für doof gehalten und absichtlich Beiträge angezeigt, die eine Nicht-Wahl nahelegen? Solche Beeinflussungen finden tatsächlich täglich statt – und ich freue mich, wenn sie funktionieren.

Meine Berufsaussichten? Super! Daten sind gefragt und zunehmend verfügbar durch diverse Online-Dienste. Was mir die Arbeit jedoch erschwert, sind Menschen, die um meine Tätigkeiten wissen und auf ihre Daten aufpassen. ●

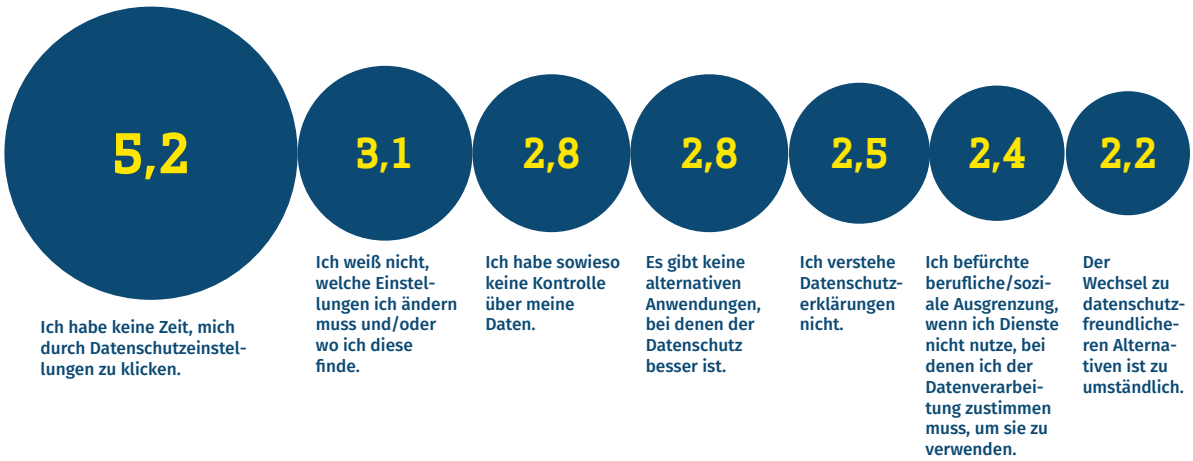
Sie haben doch nicht ernsthaft erwartet, dass Sie hier persönliche Daten über M1$c finden, oder? Datenschutz ist wichtig, das wissen Sie doch! Das Porträt wurde vom Lehrstuhl für Privatsphäre und Sicherheit in Informationssystemen an der Universität Bamberg- geschrieben.

Von unterstellter Ignoranz und systemischer Hilflosigkeit: Selbstdatenschutz zwischen Theorie und Praxis *Beitrag von Luise Kranich*

Selbstdatenschutz erfordert passende Rahmenbedingungen, geeignete Werkzeuge und viel Eigeninitiative – Nutzen und Wirkung bleiben aber häufig im Verborgenen. Ein (Er-)Klärungsversuch.

Selbstdatenschutz – was ist das eigentlich?
Eine *grundlegende* Definition des Begriffs Selbstdatenschutz finden wir in der Zielsetzung des Digital Autonomy Hubs, der u. a. Nutzer·innen dazu ermutigen und ermächtigen soll, sich mit der eigenen Datensouveränität zu beschäftigen und aktiv zu werden. Eine *engere* Definition, bei der auch die technischen, organisatorischen sowie rechtlichen Möglichkeiten und Herausforderungen konkreter sichtbar werden, begreift den Selbstdatenschutz als vornehmlich aktive Selbsthilfe oder Selbstverteidigung, – auch dann, wenn sich „Personen einem die Privatsphäre bedrohenden Umfeld gegenübersehen und ihre eigenen Datenschutzpräferenzen durchsetzen möchten“ [1]. Gerade bei der Betrachtung möglicher Hürden und Anreize wird deutlich, warum diese Unterscheidung relevant ist.

Die größte Barriere beim Schutz der eigenen Daten ist mangelnde Zeit, sich durch Datenschutzeinstellungen zu klicken.



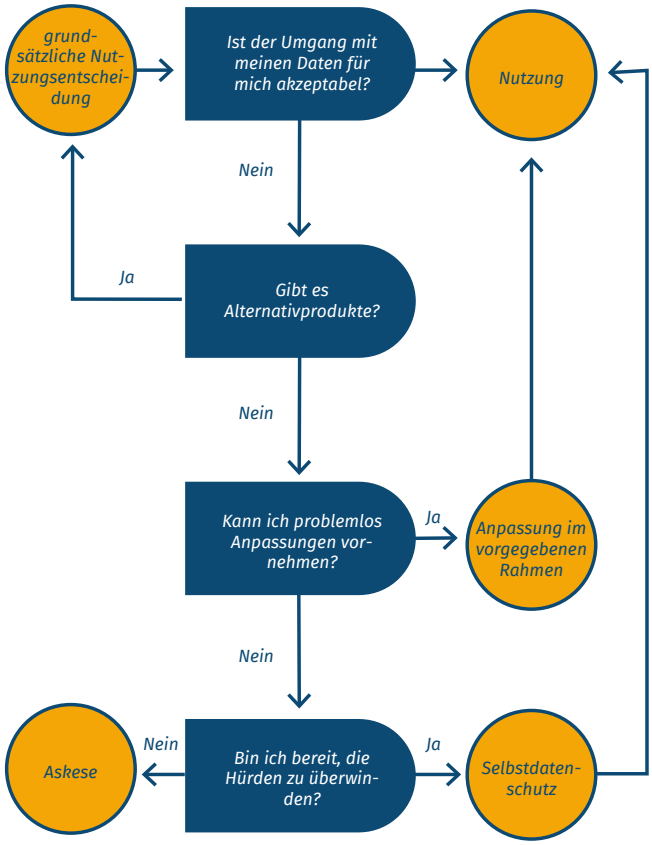
Basis: Befragte, die sich mit dem Schutz ihrer Daten mindestens etwas überfordert fühlen (n = 1620). Darstellung der Rangmittelwerte von 7 (= Anzahl der Ränge) subtrahiert. Frage Q18: Welche Dinge erschweren Ihnen den Schutz Ihrer persönlichen Daten im Alltag? Bitte ordnen Sie die folgenden Aussagen in eine Rangfolge. Bitte klicken Sie die Items nach Erschwerungsgrad an: 1 = größte Hürde, 2 = zweitgrößte Hürde etc.. © Ipsos | Digital Autonomy Hub

[1] Wagner, Manuela (2020): Datenökonomie und Selbstdatenschutz. Grenzen der Kommerzialisierung personenbezogener Daten. [1. Auflage]. Köln: Carl Heymanns Verlag (Karlsruher Schriften zum Wettbewerbs- und Immaterialgüterrecht, Band 39).

Weichenstellungen beim selbstbestimmten Umgang mit digitalen Diensten

Bei der Entscheidung zur selbstbestimmten, souveränen Nutzung digitaler Dienste stellen sich Fragen auf unterschiedlichen Ebenen. Je nach Ausgestaltung des Dienstes sind diese recht einfach zu beantworten oder bergen versteckte Hürden. Am Ende des Entscheidungsprozesses stehen im Wesentlichen drei Szenarien: Nutzung, Askese oder (aktiver) Selbstdatenschutz im engeren Sinne (s. o.). Abbildung 1 zeigt die wichtigsten Weichenstellungen auf dem Weg zu einem dieser Szenarien.

Weichenstellungen zwischen Nutzung, Askese und Selbstdatenschutz (eigene Darstellung)



A: Grundsätzliche Entscheidung über Nutzung verschiedener Produkte [2]

Frage: Möchte ich dieses Angebot (bspw. Messenger-App) nutzen?

Die vermeintlich simple Abwägung zwischen Nutzen und Risiko ist für Nutzende mit großer Unsicherheit verbunden: Das Risiko aus Datenschutzsicht ist meist nicht ohne Weiteres abschätzbar und wird vielen Menschen frühestens nach einem bekannt gewordenen Datenleck bewusst. Einen Dienst nicht zu nutzen (Abschirmung/Askese), ist dagegen häufig mit hohen (sozialen) Kosten verbunden [3] – fehlender Anschluss an ein soziales Netzwerk kann zu Isolation führen, der Verzicht auf ein smartes Thermostat zu höheren Heizkosten. Im beruflichen Kontext könnte die persönliche Präferenz für oder gegen die Nutzung eines Dienstes sogar durch Unternehmensvorgaben aufgehoben werden: Trotz DSGVO und strenger Auflagen im Beschäftigtendatenschutz fehlen in Geschäftsprozessmodellen häufig Privacy-Fragestellungen.[4]

B: Alternativprodukte

Frage: Gibt es funktional vergleichbare Produkte, die eine höhere Datensouveränität ermöglichen?

Bei einem Vergleich von Alternativen stellen sich Nutzer·innen zwei wesentliche Herausforderungen: die Informationsasymmetrie und die Kompatibilität im organisatorischen sowie technischen Sinne.

Auch für technisch Versierte ist es schwer, an relevante Informationen zu gelangen: Die Prüfung der Vertrauenswürdigkeit der Anbieter sowie die Kompatibilität mit anderen Lösungen ist häufig kaum abzuschätzen und zukünftige Änderungen durch den Anbieter sind nicht vorherzusehen, etwa der Umzug einer Smart-home-Verwaltungssoftware von einer On-Premise-Lösung in die Cloud. Insbesondere bei stark vernetzten Produkten, wie bspw. WLAN-Lautsprechern, führt eine fehlende technische Interoperabilität häufig zu Lock-In-Effekten, d. h. ein Wechsel zu anderen Anbietern ist erschwert.

C: Anpassbarkeit

Frage: Kann ich mögliche Schwachstellen mit vertretbarem Aufwand selbst beheben?

Auch wenn es der nutzenden Person gelingt, die Privatsphäre-Einstellungen eines Dienstes an die eigenen Wünsche anzupassen – bspw. durch aufwändige Neukonfiguration der Cookie-Genehmigungen einer Webseite – ist noch keine

[2] Ein ‚Produkt' kann hier ein rein digitales Produkt, z. B. eine App oder ein Online-Dienst, oder aber ein cyberphysisches System sein, also eine Kombination aus Hard- und Software.

[3] Alpers, Sascha; Betz, Stefanie; Fritsch, Andreas; Oberweis, Andreas; Schiefer, Gunther; Wagner, Manuela (2018): Citizen Empowerment by a Technical Approach for Privacy Enforcement. In: Proceedings of the 8th International Conference on Cloud Computing and Services Science. 8th International Conference on Cloud Computing and Services Science. Funchal, Madeira, Portugal, 3/19/2018 - 3/21/2018: SCITEPRESS - Science and Technology Publications, S. 589–595.

[4] Alpers, Sascha; Pilipchuk, Roman; Oberweis, Andreas; Reussner, Ralf (2018): Identifying Needs for a Holistic Modelling Approach to Privacy Aspects in Enterprise Software Systems. In: Proceedings of the 4th International Conference on Information Systems Security and Privacy. 4th International Conference on Information Systems Security and Privacy. Funchal, Madeira, Portugal, 22.01.2018-24.01.2018: SCITEPRESS – Science and Technology Publications, S. 74–82.

Datenschutz-Grundverordnung (DSGVO)

Seit 2018 ist die Datenschutz-Grundverordnung (Abkürzung: DSGVO, engl.: GDPR) in Kraft. Sie regelt die Verarbeitung personenbezogener Daten in Deutschland und allen anderen Mitgliedstaaten der Europäischen Union.

vollständig selbstbestimmte Nutzung gewährleistet. Einige Anbieter bedienen sich manipulativer Mechanismen – so genannter ‚Dark Patterns' – um Nutzer·innen unbewusst zu einem gewünschten Verhalten zu motivieren. Ein bekanntes Beispiel ist die Erzeugung eines gefühlten Termindrucks durch den Anschein einer Verknappung („x Personen sehen sich das Hotelzimmer auch gerade an").

Zuständigkeiten und Gestaltungsspielräume

Erst wenn die ersten drei Fragen in Abbildung 1 mit „Nein" beantwortet wurden und dennoch ein Wunsch zur Nutzung besteht, greift Selbstdatenschutz im engeren Sinne. Zur Lösung können verschiedene Akteure tätig werden.

D: Verantwortlichkeiten beim Umgang mit Schwachstellen

Frage: Wer initiiert systemische Anpassungen, um höhere Datensouveränität zu erreichen?

Drei Akteursgruppen können die aus ihrer Sicht notwendigen Anpassungen maßgeblich treiben: Nutzer·innen durch vorgesehene oder nicht vorgesehene Anpassungen, staatliche Initiativen zur datenschutzförderlichen Gesetzgebung und Rechtsprechung und die Anbieter technischer Selbstdatenschutzlösungen durch ergänzende Software wie Werbeblocker, die bspw. den Datenfluss zwischen dem Endgerät der Nutzer·innen und dem Online-Dienst überwachen und steuern.

IT-Industrie, Forschung, Verwaltung und Zivilgesellschaft als Treiber neuer Produktkonzepte

Ein wichtiger Beitrag des Digital Autonomy Hubs und weiterer Projekte ist es, die Akteursgruppen untereinander sowie mit den Diensteanbietern zu vernetzen und frühzeitig Anforderungen und Befürchtungen der Nutzenden in den Produktentstehungsprozess einzubeziehen. So können im Optimalfall aus Prinzipien eines reinen ‚Privacy-by-design'-Ansatzes umfassendere ‚Sovereignty-by-design'-Methoden partizipativ entwickelt und erprobt werden.

Luise Kranich,
FZI Forschungszentrum Informatik
© privat

Luise Kranich leitet am FZI Forschungszentrum Informatik die Berliner Außenstelle und den Forschungsbereich „Innovation, Strategie und Transfer". Mit ihrem Team forscht sie an technologischen, ökonomischen und gesellschaftlichen Fragen der Digitalisierung und darüber, wie Smart Data, Künstliche Intelligenz und digitale Plattformen sinnstiftend und unter Wahrung der digitalen Souveränität eingesetzt werden können.

Innovative Einblicke: DATENSPENDE

Durch die selbstbestimmte Spende der eigenen Datensätze wird nicht nur ein wichtiger Beitrag zur wissenschaftlichen Forschung geleistet, auch für Nutzer·innen werden mit innovativen Analyse- und Darstellungsformen die Wirkweise von Algorithmen, Datenverarbeitungsmechanismen und andere sonst verborgene Auswirkungen ihres digitalen Handelns erstmals nachvollziehbar gemacht.

WERTERADAR – *Gesundheitsdaten souverän spenden*

Webseite **https://werteradar.org/**

Vorhaben Das Ziel des interdisziplinären Vorhabens ist es, die Weitergabe personenbezogener Gesundheitsdaten neu zu gestalten. Damit soll Patient·innen das Spannungsfeld zwischen dem Schutz der eigenen Privatsphäre einerseits und der Bereitstellung von Daten für eine verbesserte medizinische Versorgung andererseits vor Augen geführt werden.

Zielgruppe Nutzer·innen (Patient·innen und Forscher·innen) im medizinischen Kontext

Datenspende im Projekt Das interaktive System soll es Patient·innen erlauben, über die Weitergabe ihrer persönlichen Daten zu reflektieren. Innerhalb dieses Reflexionsprozesses werden individuelle Datenschutzbedürfnisse berücksichtigt, um dem Schutzinteresse des Einzelnen durch entsprechende Vermittlungsansätze gerecht zu werden.

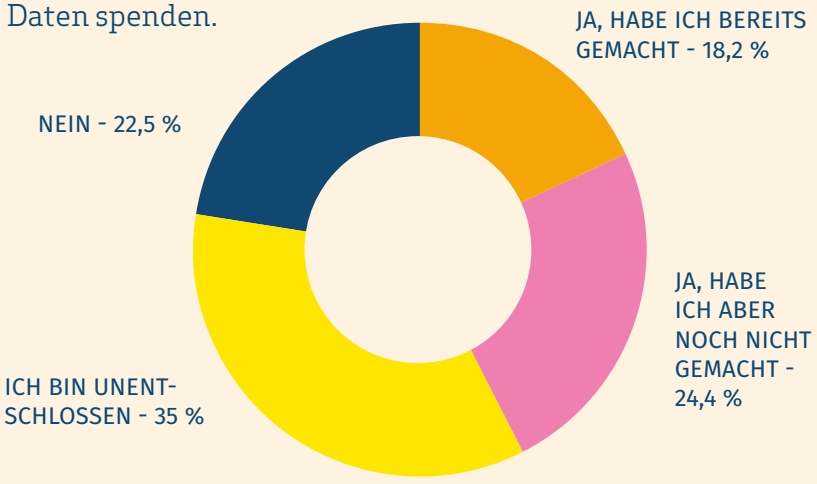
Partner Freie Universität Berlin, Fern-Universität in Hagen, Fraunhofer AISEC, Charité – Universitätsmedizin Berlin, HRTBT Medical Solutions GmbH

DATASKOP – *Was passiert mit meinen Daten?*

DataSkop

Webseite	**https://dataskop.net/**	**Datenspende im Projekt**	Datenspenden haben sich als sinnvolle Methode etabliert, um die Funktionsweise algorithmischer Systeme zu untersuchen – auch ohne direkten Zugang zu ihnen zu haben. Nutzer·innen können individuell ihre Daten spenden. Dadurch ist es möglich zu verstehen, wie die Systeme Empfehlungen, Bewertungen und Entscheidungen berechnen.
Vorhaben	DataSkop ist eine Datenspendeplattform, mit deren Hilfe algorithmische Entscheidunssysteme untersucht werden können. Durch den Einblick in diese Systeme werden Menschen befähigt, informiert mit ihren Daten umzugehen, algorithmische Strukturen zu erkennen und diese in ihren Grundzügen zu verstehen.		
Zielgruppe	Nutzer·innen generell; Forscher·innen, Journalist·innen, (Medien-) Pädaog·innen sowie die breite Öffentlichkeit.	**Partner**	AlgorithmWatch, European New School of Digital Studies, Fachhochschule Potsdam, mediale pfade – Verein für Medienbildung, Universität Paderborn

Um selbst mehr darüber zu erfahren, wie Unternehmen Daten verarbeiten, würden 43 Prozent der Befragten ihre Daten spenden.



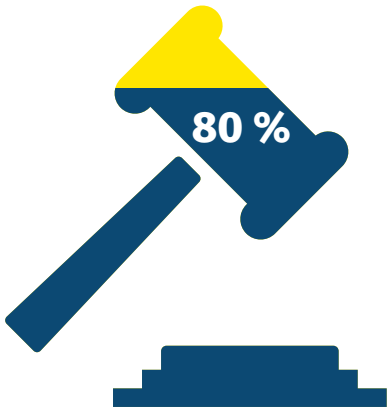
Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q11: Würden Sie pseudonymisierte oder anonymisierte Daten über Ihr digitales Nutzungsverhalten (etwa auf Webseiten oder in Apps) für Forschungszwecke zur Verfügung stellen, um selbst mehr darüber zu erfahren, wie Ihre persönlichen Daten dabei gesammelt, verarbeitet und weitergegeben werden? © Ipsos | Digital Autonomy Hub

Governance von Datenschutz
Interview mit Murat Karaboga

Knapp die Hälfte der Befragten hält in unserer repräsentativen Umfrage die aktuell geltenden Gesetze zum Datenschutz für nicht ausreichend. Macht die DSGVO Ihrer Meinung nach genügend Vorschriften für den Datenschutz?

Murat Karaboga: Die DSGVO hat ein paar Innovationen hervorgebracht, bestehende Rechte teilweise spezifiziert und sie somit an die Erfordernisse moderner Datenverarbeitungen angepasst. Sie hat aber nur unzureichend zur Überwindung des europäischen Datenschutz-Flickenteppichs beigetragen. Dies liegt daran, dass sich die Mehrzahl der EU-Mitgliedstaaten angesichts des Lobbyismus ihrer nationalen Volkswirtschaften für größere nationale Spielräume eingesetzt hat.
Grundsätzlich halte ich die DSGVO für ein aus Datenschutzperspektive sinnvolles Gesetz, das aber vielmehr einen ersten wichtigen Schritt darstellt, auf den weitere folgen müssen. Schließlich regelt die Verordnung vor allem das Grundsätzliche in Bezug auf den Datenschutz. Spannend wird es aber erst dann, wenn einzelne riskante Bereiche, in denen Daten verarbeitet werden, näher in den Fokus der Betrachtung rücken, etwa Social-Media-Plattformen oder KI-Anwendungen. Hier sind Spezialgesetze erforderlich, die auf den Grundprinzipien der DSGVO beruhen und diese in die Praxis überführen.

80 % der Befragten halten Datenschutz nur durch strengere Gesetze für möglich.



Basis: alle Befragten (n = 2000). Darstellung der Top 2. Angaben in Prozent. Frage Q19: Inwiefern stimmen Sie den folgenden Aussagen zu? Anbieter·innen von digitalen Geräten und Anwendungen können nur durch strengere Gesetze zum datenschutzfreundlichen Handeln gebracht werden.

In unserer Umfrage haben 80 % der Befragten den Eindruck, dass Anbieter von digitalen Geräten und Anwendungen nur durch strengere Gesetze zum datenschutzfreundlichen Handeln gebracht werden können. Was sind denn aktuelle politische Vorstöße für einen besseren Datenschutz?

Diesen Eindruck kann ich nur unterstreichen, denn meist bedeuten mehr Daten auch mehr Einnahmen für die Anbieter. Der Wettbewerbsdruck erschwert ethische Datenverarbeitungen, denn wer nicht mitzieht, droht wirtschaftlich ins Hintertreffen zu geraten. Öffentlicher Aufschrei ist relevant, um bestimmte fragwürdige Verarbeitungspraktiken zu kritisieren, kann aber immer nur punktuell geschehen. Nur regulatorische Vorschriften, die auch durchgesetzt werden, schaffen eine Lösung in der Breite. Aktuell gibt es drei politische Vorstöße: zum einen die stagnierende Überarbeitung der ePrivacy-RL zur ePrivacy-VO. Außerdem die EU-KI-Regulierung, die gewissermaßen als Ausfluss aus der DSGVO für den KI-Bereich gelesen werden kann, aber auch darüber hinausgeht. Schließlich kann auch der Regulierungsvorschlag zum Digital Services Act der EU (im weiteren Sinne auch der Digital Markets Act der EU) als Ausfluss aus der DSGVO für den Bereich von Social-Media-Plattformen gelesen werden.

In unserer Studie stimmten 87 % der Befragten der Aussage zu, dass Geräte und Apps stets die datenschutzfreundlichsten Einstellungen als Voreinstellungen haben sollten. Halten Sie den Ansatz Privacy by Default (PbD) für durchsetzbar?

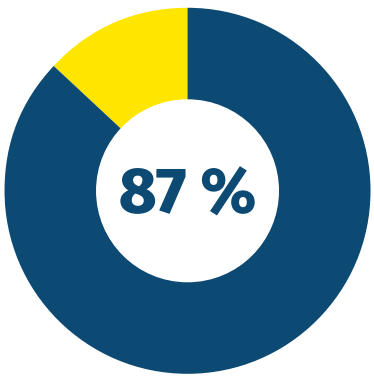
Die Schwierigkeit bei dem Ansatz des PbD ist die Definition des Default-Status. Als der Ansatz mal entwickelt wurde, war ein datensparsamer Default-Standard Ausgangspunkt des Konzepts. Basierend auf den datensparsamsten Einstellungen eines Dienstes sollten Nutzer·innen selbständig weitere Datennutzungen freigeben können, ohne dass sie dazu gezwungen oder ‚genudget' werden. Die Erstellung eines Profils bei einem Social-Media-Diensteanbieter sollte beispielsweise nicht dazu führen, dass die Profil-Einstellun-

gen von vornherein auf öffentlich gesetzt sind. Dieses Verständnis wurde so auch von der Datenschutz-Forschungscommunity geteilt und weiterentwickelt.

Wie hat sich die Definition von PbD dann verändert?

Während der Verhandlungen zur DSGVO demonstrierten datenverarbeitende Unternehmen stark gegen ein derartiges PbD-Verständnis. Das zentrale Argument lautete, dass Betroffene im Rahmen der Nutzung eines Dienstes selbst festlegen sollten, was Default bedeutet. Der Default-Standard sollte also an den Nutzungszweck gekoppelt werden, der wiederum von den datenverarbeitenden Stellen festgelegt wird. Dieses Verständnis hat dann auch Eingang in die DSGVO gefunden. Als Default gilt, wozu Betroffene eingewilligt haben bzw. was der rechtmäßige Zweck der Verarbeitung ist. Somit können selbst sehr weitgehende Datenverarbeitungen als konform mit PbD definiert werden.

Fast 9 von 10 Personen sprechen sich für Privacy by Default aus.



Basis: alle Befragten (n = 2000). Darstellung der Top 2. Angaben in Prozent. Frage Q22: Inwiefern stimmen Sie der folgenden Aussagen zu? Geräte und Apps sollten immer die datenschutzfreundlichsten Einstellungen als Voreinstellungen haben. © Ipsos | Digital Autonomy Hub

ePrivacy-Richtlinie und -Verordnung:

Die ePrivacy-Richtlinie (ePrivay-RL) regelt den Datenschutz in der digitalen Kommunikation in der Europäischen Union. Es wird darüber verhandelt, sie durch eine ePrivacy-Verordnung (ePrivacy-VO) zu ersetzen. Anders als eine Richtlinie gilt eine Verordnung verbindlich und unmittelbar in den Mitgliedsstaaten der Europäischen Union.

Nichtsdestotrotz haben sich viele Diensteanbieter im Laufe der Jahre angesichts der öffentlichen Proteste gegen weitgehende Datenverarbeitungen zunehmend datenschutzfreundlicher aufgestellt. Die Einrichtung eines Social-Media-Profils z. B. führt bei vielen Diensten inzwischen nicht mehr zu einer automatischen Veröffentlichung aller Inhalte. Dies ist sehr zu begrüßen. Diese Handlungen sind jedoch meist „good will" und keine Verpflichtung. Hier wäre eine stärkere gesetzliche Definition des Default-Standards sehr zu begrüßen.

Welche politischen und rechtlichen Möglichkeiten wären außerdem denkbar?

Die Technologie- und Dienste-Entwicklung bleibt nicht stehen. Neue Angebote und die zunehmende Ausstattung vieler Lebensbereiche des Menschen mit digitaler Sensorik, zum Beispiel durch Smart Wearables und Smart-home-Geräte, schaffen immer wieder neue Herausforderungen für den Datenschutz. Da müssen EU- und nationale Gesetzgeber mithalten können. Wichtig wäre es, neben den oben genannten Gesetzesinitiativen stets auch weitere risikoadäquate Regulierungen voranzutreiben, wann immer dies erforderlich ist. Der Europäische Datenschutzausschuss veröffentlicht in regelmäßigen Abständen Empfehlungen zur Operationalisierung der vergleichsweise abstrakten DSGVO-Vorgaben im Hinblick auf verschiedene Datenverarbeitungskontexte. Dies könnte ein guter Anknüpfungspunkt sein. Aber auch die Zivilgesellschaft und Wissenschaftscommunity entwickeln laufend sinnvolle Vorschläge, die stärker beachtet werden sollten.

Murat Karaboga, Fraunhofer Institut für System- und Innovationsforschung ISI / Forum Privatheit
© Franz Warmhof Fraunhofer ISI

Murat Karaboga ist Politikwissenschaftler und arbeitet seit 2014 am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. In seiner Forschung untersucht er, wie neue Technologien ihren Weg in die Gesellschaft finden können, ohne negative Nebeneffekte mit sich zu bringen. Seiner kürzlich abgeschlossenen Promotion behandelt die Entstehung der DSGVO unter Berücksichtigung der Datenschutzwahrnehmungen der beteiligten Akteure.

Tipps zum Selbstdatenschutz
Beitrag von Bettina Müller

Mit Selbstdatenschutz sind Maßnahmen gemeint, die ich treffe, um meine informationelle Selbstbestimmung zu sichern. Ich will wissen und kontrollieren, wer welche persönlichen Daten wann, wo und zu welchem Zweck erhebt, nutzt oder weitergibt. Dieses Grundrecht wird bei fast jeder Aktivität in der digitalen Welt angegriffen. Nicht nur kriminellen Attacken – durch Viren, Hoax, Phishing etc. – bin ich ausgesetzt. Auch Anbieter greifen im breiten Stil auf meine Daten zu, sammeln Informationen über mein Verhalten, meine Beziehungen, aber auch meine Kontaktpersonen in der digitalen Welt.
Kurz und kompakt folgen nun einige Tipps und Strategien zur eigenen Anwendung:

Software:
· Cloudsoftware, Online-PDF-Tools und Online-Speicher vermeiden
· quelloffene Software verwenden
· Funktionen reduzieren, z. B. PDF-Reader verwenden, die – nur die Anzeige von Dokumenten ermöglichen

Internet:
· unerwünschte Seiten in der hosts-Datei nach 0.0.0.0 oder 127.0.0.1 bzw. IP-6-Äquivalenten „umleiten“; zu Hause einen eigenen Proxy (es reicht ein Raspi) einsetzen
· neutrale DNS-Server nutzen
· Internetzugang für ausschließlich im Heimnetz genutzte Geräte (z. B. Drucker) im Router blockieren und Drucker über IP, nicht über Webdienste, anbinden

E-Mail:
· „echte“ E-Mail-Adressen schützen durch „Wegwerf-E-Mail-Adressen“
· E-Mail-Client nutzen anstatt Webmail
· keine Dienste nutzen, die Adressbücher in der Cloud speichern, denn damit wandern auch die Adressen der Mailpartner in die Cloud
· E-Mail primär als reinen Text betrachten, dann fallen gefälschte Links schneller auf
· keine Dateien/Bilder aus dem Internet nachladen (ausschließlich Mailanhänge nutzen)

Die Befragten treffen verschiedene Maßnahmen, um ihre Daten zu schützen.

64 % Ich verwende verschiedene Passwörter für verschiedene Dienste.
58 % Ich lösche Daten über meine Onlineaktivitäten (z. B. Browserverläufe, Cookies).
48 % Ich vermeide bestimme Anbieter.
39 % Ich lehne bei Cookie-Bannern auf Internetseiten die Cookies zu Marketingzwecken ab, inklusive jener, die sich unter dem Abschnitt ‚Berechtigtes Interesse‘ befinden.
37 % Ich konfiguriere die Einstellungen bei meinen Geräten und Anwendungen so, dass der Zugriff auf sensible Daten verwehrt wird.
26 % Ich nutze verschlüsselte Kommunikation.
18 % Ich nutze ein VPN.
12 % Ich nutze datenschutzfreundliche Alternativen zu verbreiteten Geräten und Anwendungen.

Basis: Befragte, die Maßnahmen zum Schutz ihrer Daten umsetzen (n = 1960). Angaben in Prozent. Frage Q15: Welche Maßnahmen treffen Sie, um Ihre Daten zu schützen? © Ipsos | Digital Autonomy Hub

· datenschutzfreundliche Provider verwenden
· E-Mails mittels MIME oder OpenPGP verschlüsseln
· Beim Versenden von E-Mails an feste Gruppen keine langen CC-Listen verwenden, sondern Mailinglisten anlegen, bei denen alle Teilnehmer eine eigene E-Mail erhalten

Smartphone:
· Funktionen wie Standort, Bluetooth und mobile Daten nur anschalten, wenn diese wirklich genutzt werden
· verschiedene Geräte nicht im Netz synchronisieren
· Smartphone rooten, ein alternatives Betriebssystem verwenden,
· VPN-Verbindung und Adblocker nutzen
· freie App-Stores verwenden
· Prepaid-Karten aus Tauschbörsen verwenden
· keine besonders vertraulichen Anwendungen auf dem Smartphone nutzen (etwa hinsichtlich Gesundheit, Finanzen)

Social Media:
· Messenger nicht mit der Telefonnummer verbinden, sondern dezentrale, anonym nutzbare Messenger mit Pseudonymen verwenden
· keine Cloudspeicher nutzen: Adressbücher, Favoriten, Passwörter etc. nicht zentral ablegen

Surfen:
· datenschutzfreundliche Suchmaschine verwenden
· Skripte von Dritten[5] unterbinden und ggf. in getrennter Browserumgebung temporär freigeben
· datenschutzfreundliche Browser verwenden[6]
· Tracking und Werbung blockieren[7]
· datenschutzfreundliche Browser bzw. mehrere Browser für verschiedene Zwecke und isolierte Container verwenden

Eine gute Übersicht mit Tipps zur digitalen Selbstverteidigung findet sich außerdem unter digitalcourage.de!

63 % der Befragten finden, dass Nutzer·innen selbst die Verantwortung dafür tragen, ihre Daten zu schützen.

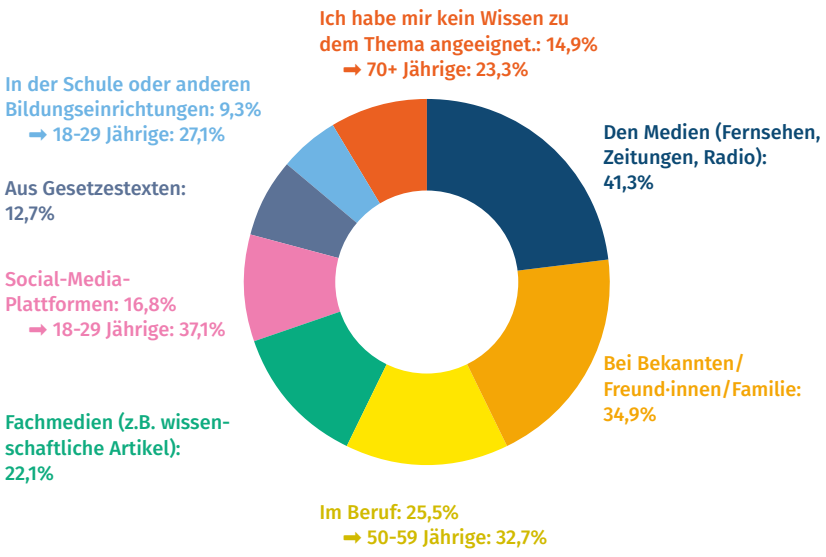
Bettina Müller ist ein digitales Urgestein: Bereits 1967 lernte sie im Informatikunterricht in der Schule an einer Zuse Z23. Sie studierte Medizin (Approbation und Promotion), Mathematik, Informatik und Medizinrecht (LL.M.). Seit 1987 ist sie im Netz unterwegs und seit 1995 Mitglied im Präsidiumsarbeitskreis der GI. Die Ärztin und ausgebildete Datenschutzbeauftragte ist außerdem Mitglied im BvD und im Chaos Computer Club.

[5] https://de.wikipedia.org/wiki/NoScript
[6] https://www.datenschutzexperte.de/blog/datenschutz-im-unternehmen/browser-datenschutz-welcherbrowser-schuetzt-ihre-daten/
[7] https://de.wikipedia.org/wiki/UBlock_Origin

3/ DIGITALE KOMPETENZEN

Digitale Kompetenzen bezeichnen in ihrem Kern Fähigkeiten und Wissen, die ein Mensch benötigt, um kompetent, selbstorganisiert und souverän im digitalen Raum zu handeln, sich mit Technologien auseinandersetzen und diese nutzen zu können. Diese können für unterschiedliche Gruppen der Gesellschaft jedoch verschiedene Dinge bedeuten und der individuelle Kompetenzaufbau steht immer in Abhängigkeit der eigenen Bedürfnisse, Hürden und Chancen. In diesem Kapitel werden der Erwerb und der Nutzen digitaler Kompetenzen aus den Perspektiven verschiedener Altersgruppen beleuchtet

Die Befragten informieren sich auf vielfältige Weise darüber, wie sie ihre Daten schützen können.



Basis: alle Befragten (n=2.000). Angaben in Prozent. Frage Q21c: Wo haben Sie sich Ihr Wissen darüber angeeignet, wie Sie Ihre Daten bei der Nutzung von Geräten und Apps schützen können? Bitte klicken Sie alle zutreffenden Optionen an. © Ipsos | Digital Autonomy Hub

Zwischen Autonomie und Schutzbedarf – Kinder in einer von digitalen Medien geprägten Welt

Beitrag von Jutta Croll, Dr. Jan-Christoph Heilinger und Prof. Dr. Saskia K. Nagel

Kinder kommen heute in immer jüngerem Alter mit digitalen Diensten und Endgeräten in Kontakt. Smartphone, Tablet und Apps sind vertraute Alltagsbegleiter und selbst im Zimmer von Kleinkindern sind vernetzte Spielzeuge und digitale Geräte zur Kontrolle von Körperfunktionen keine Seltenheit. Dabei entsteht ein Spannungsfeld von Schutz- und Freiheitsrechten, das die Wahrung von Datenschutz und Privatsphäre einerseits sowie von Autonomieansprüchen andererseits vor Herausforderungen stellt.

Schutz und Befähigung

Digitale Technologien sind in den heutigen Gesellschaften ubiquitär und finden zunehmend auch Einzug in die Kinderzimmer. Schon Kleinkinder sind von den leuchtenden, blinkenden und tönenden Geräten fasziniert. Angesichts der stimulierend wirkenden Screens besteht eine Herausforderung darin, die nachwachsende Generation zu kompetenten Nutzer·innen digitaler Technologien zu machen und sie dazu zu befähigen, die damit einhergehenden Vorteile genießen zu können. Daraus ergibt sich die Aufgabe, den Einfluss von digitalen Technologien auf das Verhalten von Kindern zu verstehen und den Zugang pädagogisch zu begleiten sowie ggf. auch zu begrenzen.

Um von den Chancen der Digitalisierung auch langfristig profitieren zu können, ist es erforderlich, dass die Nutzer·innen digitaler Technologien über ein Mindestmaß an Medien- und Nutzungskompetenz verfügen. Auch Erwachsene haben häufig Schwierigkeiten, sich im digitalen Bereich kompetent zu bewegen, redaktionelle Inhalte von Werbung zu unterscheiden und den eigenen Medienkonsum reflektiert zu regulieren. Der Einfluss und die Attraktivität digitaler Angebote ist groß, insbesondere wenn diese sich auf soziale Bedürfnisbefriedigung konzentrieren, wie z. B. in den sozialen Medien. Werbung und kommerzielle Interessen bedienen sich gezielt dieser Dynamiken, um Aufmerksamkeit zu erlangen bzw. zu erhalten und gezielt Verhaltensänderungen bei den Nutzenden digitaler Technologien herbeizuführen. Wenn schon Erwachsene diese Schwierigkeiten erleben, ist es ungleich schwieriger für Kinder, sich diesbezüglich kompetent zu verhalten. Deshalb war eine zeitgemäße Jugendschutzgesetzgebung, wie sie zum 1. Mai 2021 novelliert in Kraft getreten ist, überfällig.

Daneben sind auch Datenschutzregelungen wichtig, um die Privatsphäre und Kontrolle über persönliche Daten auch für die besonders schutzbedürftigen Minderjährigen zu sichern. Dem trägt die europäische Datenschutzgrundverordnung mit einem altersdifferenzierenden Ansatz erstmals Rechnung. Sie nimmt dabei Bezug auf die UN-Kinderrechtskonvention, die nach dem Prinzip der sich bei Kindern entwickelnden Fähigkeiten ausdrücklich alters- und entwicklungsangemessene besondere Schutz-, Befähigungs- und Freiheitsrechte für junge Menschen von der Geburt bis zum 18. Lebensjahr vorsieht.

Datenschutz und Kinderrechte

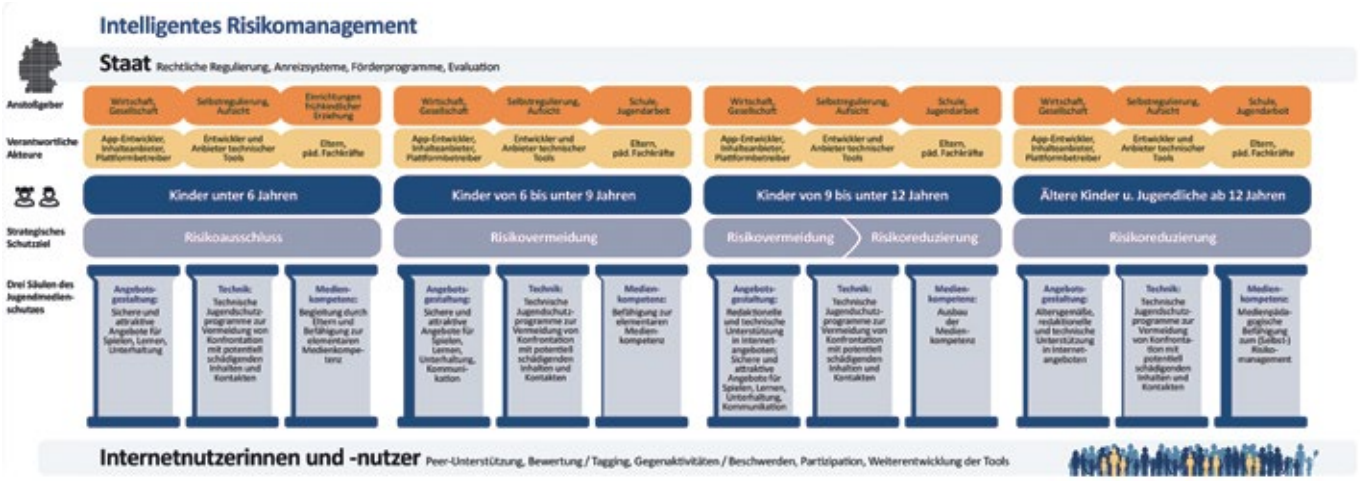
Die Rechte von Kindern sind seit 1989 in der UN-Kinderrechtskonvention festgeschrieben. Das Internet steckte damals noch in den Kinderschuhen, daher ist es nicht verwunderlich, dass es in der Konvention noch keine Erwähnung findet. Wie die Freiheits- und Schutzrechte von Kindern im Zuge der digitalen Transformation der Gesellschaft neu zu verstehen sind und welche Maßnahmen erforderlich sind,

um die Kinderrechte zu gewährleisten, beschreibt die 25. Allgemeine Bemerkung zur UN-KRK[8], die im März 2021 vom Kinderrechteausschuss der Vereinten Nationen veröffentlicht wurde.

Digitalisierung kann dazu beitragen, dass Kinder ihre Rechte auf Zugang zu Informationen, auf freie Meinungsäußerung, Versammlung und Vereinigung besser wahrnehmen können; die Handlungsfähigkeit von Kindern – im Englischen als Agency bezeichnet – und ihre Autonomie können dadurch gestärkt werden. Gleichzeitig resultiert aus der Nutzung digitaler Dienste durch Kinder in vielen Bereichen ein erhöhtes und teilweise noch nicht ausreichend verstandenes Gefährdungspotenzial, dem durch geeignete Schutzmaßnahmen (s. JuSchG) entgegenzuwirken ist. Das Recht auf Privatsphäre und Datenschutz gem. Art. 16 der UN-KRK ist direkt in diesem Spannungsfeld angesiedelt. Einige der Regelungen der Datenschutz-Grundverordnung greifen ein in den Autonomieanspruch von Kindern und Jugendlichen. Hier ist vorrangig die in Art. 8 DSGVO geforderte Einwilligung der Erziehungsverantwortlichen in die Nutzung von Diensten der Informationsgesellschaft durch unter 16-Jährige zu nennen, bei der den Schutzinteressen Vorrang gegeben wird gegenüber den Freiheitsrechten der Kinder. Wenn es um die Inanspruchnahme von Online-Beratungsdiensten geht, steht diese Regelung der DSGVO in direktem Widerspruch zu § 8 SGB VIII, der Kindern einen Anspruch auf Beratung ohne Kenntnis des Personensorgeberechtigten gewährt. Gesundheitsdaten sind nach Art. 9 des DSGVO als sensible Daten zu kategorisieren, sie unterliegen somit einem noch höheren Schutzniveau. Dieses ist durch die Anbieter entsprechender Dienste zu gewährleisten, aber auch durch Erziehungsverantwortliche, die mit entsprechenden Geräten – z. B. Teddy the Guardian[9] – solche Daten ihrer Kinder erheben. Erziehungsverantwortliche verfügen aber potenziell auch selbst nicht über genügend Informationen und Medienkompetenz für den geforderten sorgsamen Umgang mit Geräten und den dadurch verarbeiteten sensiblen Daten.

Fazit: Autonome Nutzung lernen

Damit Menschen selbstbestimmt über ihre eigene Mediennutzung entscheiden und dauerhaft die Vorteile digitaler Technologien nutzen können, müssen sie die Möglichkeit haben, ihre Kompetenzen und Orientierungsfähigkeiten frühzeitig zu entwickeln, um diese auch im Umfeld digitaler Technologien anwenden zu können. Für junge Menschen ist eine Differenzierung nach Altersgruppen erforderlich, wie sie 2016 am Zentrum für Kinderschutz im Internet mit dem Modell des Intelligenten Risikomanagements[10] entwickelt wurde. Das Modell sieht für die jüngste Altersgruppe der Kinder unter sechs Jahren den Ausschluss von Risiken vor, mit zunehmendem Alter sind Risikovermeidung und für die Jugendlichen Risikoreduzierung die strategischen Schutz-



Modell Intelligentes Risikomanagement, ©Zentrum für Kinderschutz im Internet, 2016

[8] https://kinderrechte.digital/hintergrund/index.cfm/topic.280/key.1661 (zuletzt aufgerufen am 21.08.2021).

[9] https://de-de.facebook.com/TeddyTheGuardian/.

[10] Der Begriff stützt sich auf die Evaluation des Jugendschutzsystems in Deutschland, die 2006/2007 vom Hans-Bredow-Institut vorgenommen wurde: https://www.hans-bredow-institut.de/de/projekte/analyse-des-jugendmedienschutzsystems-jugendschutzgesetz-und-jugendmedienschutz-staatsvertrag (zuletzt aufgerufen am 21.08.2021) sowie https://kinderrechte.digital/hintergrund/index.cfm/topic.279/key.1497 (zuletzt aufgerufen am 21.08.2021).

ziele. Die Schutzmaßnahmen umfassen medienpädagogische Begleitung und Unterstützung sowie die Befähigung zum Selbstschutz für die älteren Kinder, kind- und jugendgerechte Angebotsgestaltung sowie technische Schutzmaßnahmen insbesondere für jüngere Kinder.
Mit einem so gestalteten holistischen Ansatz kann dem Vorrang des Kindeswohls als oberstes Prinzip der UN-Kinderrechtskonvention Rechnung getragen werden und ein gutes Aufwachsen mit Medien ebenso wie ein souveräner und autonomer Umgang mit Technik können für alle Altersgruppen erreicht werden.

Jutta Croll
Stiftung Digitale Chancen
© Mark Bollhorst

Jutta Croll ist Vorstandsvorsitzende der Stiftung Digitale Chancen, einer gemeinnützigen Organisation mit dem Auftrag, die gesellschaftlichen Folgen der Digitalisierung zu erforschen, sich für den chancengleichen Zugang aller Menschen zum Internet einzusetzen und ihre Medienkompetenz zu stärken. Jutta Croll ist bei der Stiftung verantwortlich für das auf internationale Zusammenarbeit ausgerichtete Projekt Kinderschutz und Kinderrechte in der digitalen Welt (www.kinderrechte.digital.)

Dr. Jan-Christoph Heilinger,
RWTH Aachen, Angewandte Ethik,
© Michael McKee

Jan-Christoph Heilinger ist Postdoctoral Researcher and Lecturer in Philosophie an der RWTH Aachen. Seine Forschungsinteressen liegen in der praktischen Philosophie, insbesondere in der anwendungsbezogenen Ethik und der politischen Philosophie.

Prof. Dr. Saskia K. Nagel,
RWTH Aachen, Angewandte Ethik
© Saskia K. Nagel

Prof. Dr. Saskia Nagel ist Universitätsprofessorin für Angewandte Ethik an der RWTH Aachen. Sie hat Cognitive Science und Philosophie studiert und arbeitet an der Schnittstelle von Ethik, Philosophie, Lebens- und Technikwissenschaften in interdisziplinären Teams. Sie untersucht, wie neue Mensch-Technik-Beziehungen das Selbstverständnis und das Werteverständnis des Menschen beeinflussen.

Innovative Einblicke: GAMIFICATION

Gamification ist die Übertragung von Spielprinzipien in eine spielfremde Umgebung. Der Spieltrieb kann Menschen aller Altersstufen dazu motivieren, selbst komplexe oder als unangenehm empfundene Aufgaben leichter zu erledigen. In der Mensch-Technik-Interaktion können über Gamification Anreize geschaffen werden, um Menschen verschiedener Altersstufen und verschiedener Technikaffinität dabei zu unterstützen, sich digitale Kompetenzen zu erarbeiten und sich souveräner in der digitalisierten Welt zu bewegen.

A-DIGIKOMP – *Digitale Kompetenz und Souveränität Adoleszenter durch Micro Games adaptiv fördern*

A-DigiKomp

Webseite www.a-digikomp.rwth-aachen.de

Vorhaben Ein digitaler Assistent und Serious Game liefern ein bedarfsorientiertes Angebot, mit dem adoleszenten Nutzer·innen ihre Digitalkompetenzen trainieren können. Die Spielinhalte umfassen verschiedene Rechtsbereiche sowie Ereignisse im digitalen Raum, beziehen Erfahrungen der Zielgruppe mit ein und decken Denkfehler auf.

Zielgruppe Die Zielgruppe von A-DigiKomp sind adoleszente Nutzer·innen.

Gamification im Projekt Das Serious Game ermöglicht spielerischen Kompetenzerwerb, der auf den Alltag Adoleszenter im digitalen Raum abgestimmt ist. Innerhalb der Spielwelt werden die Spieler·innen mit Ereignissen im digitalen Raum konfrontiert und erhalten Handlungsalternativen. Sie können so in einem geschützten Raum kompetentes Handeln trainieren.

Partner HSD Hochschule Döpfer gGmbH, imc information multimedia communication AG, Promotion Software GmbH - Serious Games Solutions, Rheinisch-Westfälische Technische Hochschule Aachen, Technische Universität Kaiserslautern, Universität des Saarlandes

EPA-COACH – *Digitale Souveränität für Senioren mit der elektronischen Patientenakte*

Webseite **https://epacoach.de/**

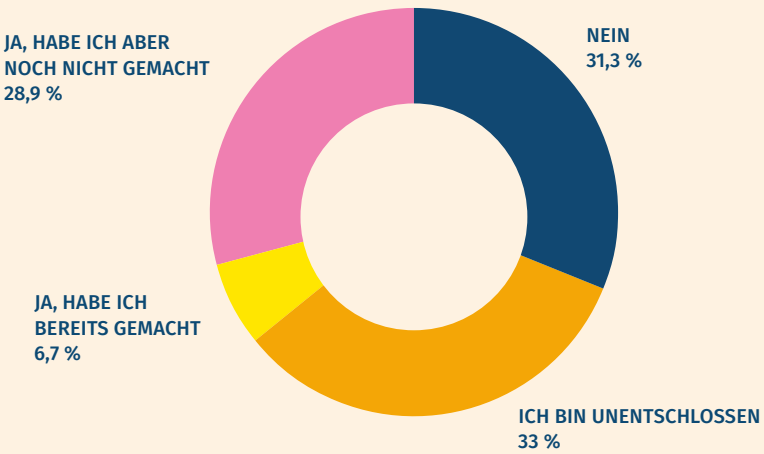
Vorhaben Innerhalb einer E-Learning-Plattform können ältere Menschen den souveränen Umgang mit der elektronischen Patientenakte spielerisch erlernen. Dabei werden nicht nur Inhalte erläutert, sondern auch Kompetenzen vermittelt, z. B. das Verwalten von Daten und digitalen Inhalten in der ePa oder das Schützen der Privatsphäre und der Gesundheitsdaten.

Zielgruppe Die Zielgruppe bilden ältere Menschen (Alter > 65 Jahre), die Interesse daran haben, die elektronische Patientenakte zu nutzen und mehr dazu erfahren möchten.

Gamification im Projekt Das Gamification-Konzept im Projekt besteht aus Ansätzen zur Steigerung der spezifischen Lernmotivation der Zielgruppe und basiert auf dem Octalysis Framework von Chou (2021). Der Gamification Basisansatz bezieht sich auf vier Kernantriebe: Entwicklung und Leistung, epische Bedeutung, Befähigung von Kreativität und sozialer Einfluss.

Partner Beuth Hochschule für Technik Berlin, Charité - Universitätsmedizin Berlin, Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Rheinisch-Westfälische Technische Hochschule Aachen, The People Who Do TPWD GmbH

Spiele spielen für mehr Datenschutz-Kompetenz?



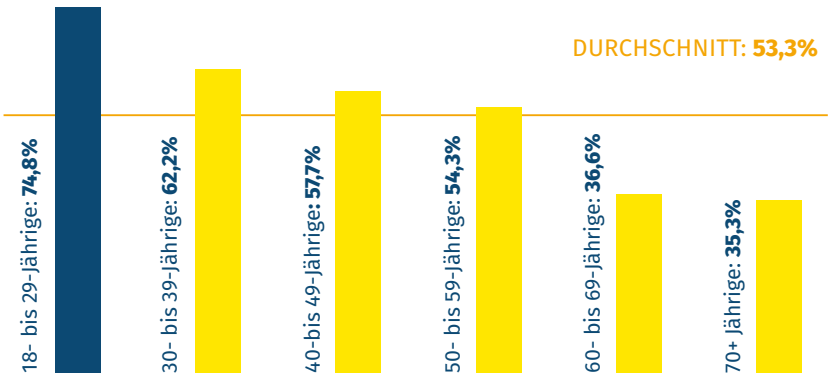
Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q27: Würden Sie ein gratis Online-Spiel spielen, um Ihr Wissen und Ihre Kompetenzen im Datenschutz zu verbessern? © Ipsos | Digital Autonomy Hub

Junge Generationen zwischen sozialer Teilhabe und Datenschutz *Interview mit Dr. Johanna Schäwel*

Was bedeutet digitale Souveränität in einem medienpsychologischen Kontext?

Dr. Johanna Schäwel: Souveränität an sich bedeutet Selbstbestimmtheit und die Freiheit, so zu handeln, wie man handeln möchte. Insbesondere im Bereich der digitalen Medien geht es um Datensouveränität – die Kontrolle über den Umgang mit den eigenen Daten. Diese Selbstbestimmung ist sehr wichtig, weil sie Menschen ein Gefühl von Autonomie gibt, was sich positiv auf das eigene Wohlbefinden auswirkt. Im medienpsychologischen Kontext ist also mit Souveränität selbstbestimmtes Handeln mit und in (sozialen) Medien gemeint. Wenn wir Kontrolle darüber haben, wer die Daten, die wir in sozialen Medien verbreiten oder hinterlassen, auf welche Weise benutzt, sind wir souverän und selbstbestimmt. Natürlich ist das nicht immer möglich, aber wir streben danach. Damit kommen wir auch zum Stichwort Medienkompetenz: Es umfasst sowohl Selbstbestimmtheit als auch Kritikfähigkeit bezüglich des Konsums und der Erstellung von Medien.

Wer schätzt die eigene digitale Kompetenz gut bis sehr gut ein?



Basis: alle Befragten (n = 2000). Darstellung der "Noten" 1 und 2. Angaben in Prozent. Frage Q2. Wie schätzen Sie Ihre eigene Kompetenz im Umgang mit digitalen Geräten und Anwendungen ein? Bitte bewerten Sie Ihre Kompetenz auf einer Skala von 1 bis 6, auf der 1 „sehr gut" und 6 „sehr schlecht" heißt. © Ipsos | Digital Autonomy Hub

Junge Erwachsene verfügen über hohe digitale Kompetenzen und breites Wissen rund um den Datenschutz. Dennoch gibt die Mehrheit zu, Apps und Geräte mit mangelndem Datenschutz zu nutzen. Ein wesentlicher Faktor ist hier die Furcht vor sozialem Ausschluss – überrascht Sie das?

Nein, das überrascht mich nicht. Was ich zunächst noch wichtig finde, ist die Unterscheidung zwischen digitalen Kompetenzen im Sinne der Mediengestaltung und Wissen über Datenschutzpraktiken. Viele junge Menschen wissen, wie sie ihre TikTok-Videos schneiden oder wie sie Instagram-Postings optimieren, aber das heißt nicht, dass sie auch über Datenschutz Bescheid wissen. Zudem stellt sich die Frage, wie verlässlich die Selbstauskunft über die eigene Medienkompetenz ist: Können Jugendliche wirklich einschätzen, ob sie gut informiert sind oder glauben sie das nur? Wir brauchen Skalen, die Medienkompetenz umfassend und gut abbilden.
Bei der konkreten Nutzung von digitalen Anwendungen überwiegt häufig das Bedürfnis nach sozialer Teilhabe und Datenschutzbedenken rücken in den Hintergrund. In erster Linie geht es hier um den Austausch mit anderen Menschen,

Kommunikation und Unterhaltung. Das ist natürlich greifbarer und erstrebenswerter, als über langfristige Konsequenzen nachzudenken, die negativ sein können, aber in dem Moment nicht so sichtbar sind. Aus der Psychologie wissen wir auch, dass Einstellungen und Wissen nicht direkt zum Handeln führen. Je nach Handlungsintention und situativen Kontextfaktoren kommt es dann vor, dass wir solche Anwendungen benutzen, obwohl wir eigentlich um deren Bedenklichkeit wissen. Kompetenz ist also wichtig, aber nicht der alleinige Faktor.

Warum ist gerade den jüngeren Generationen soziale Teilhabe so viel wichtiger als der Schutz der eigenen Daten?

Gerade für junge Menschen ist soziale Teilhabe wichtig, weil man sich insbesondere als junger Mensch noch im Findungsprozess befindet. Als wichtiger Bestandteil der Identitätsentwicklung vergleicht man sich gerne mit anderen Menschen, tauscht sich aus, sucht nach sozialer Unterstützung, nach Kontakt, nach Rückmeldung und auch nach Kreativität. Man möchte sich kreativ ausleben und verschiedene Dinge ausprobieren. All das kann man in den sozialen Medien super machen, sie bieten sehr viel Potenzial für Kommunikation und Kreativität.

Muss es immer so laufen? Wie können wir dafür sorgen, dass Menschen der Schutz der eigenen Daten genauso wichtig ist wie die Teilnahme an sozialen Medien?

Das ist eine schwierige Frage, mit der sich verschiedene Disziplinen beschäftigen. Generell gesagt ist es wichtig, Reflexionsprozesse anzustoßen und kritische Reflexion zur Routine werden zu lassen. Ein guter Weg ist es, verständlich sowie – besonders wichtig – auf kompakte und nicht zu komplexe Weise zu erklären, wie digitale Anwendungen funktionieren, etwa wie bestimmte Apps arbeiten. Außerdem ist es zielführend, datenschutzfreundliche Alternativen aufzuzeigen. Es ist wichtig, Datenschutz und Medienkompetenz nicht als Gegenpol zu Mediengenuss zu sehen. Häufig besteht nämlich die Angst, entweder Medien hervorragend nutzen und sich austauschen zu können – oder die eigenen Daten zu schützen. Es geht aber auch beides. Medien können und sollen fürs Vergnügen, für Austausch, für Informationsrecherche herangezogen werden, wichtig sind dabei aber die Rahmenbedingungen und welche Anwendung ich mit welchen Einstellungen nutze.

Gibt es einen konkreten Tipp für den Alltag, den Sie uns mitgeben würden? Wie könnten wir beispielsweise unsere Geschwister, Kinder oder unseren Freundeskreis sensibilisieren?

Das Problem ist natürlich, dass die meisten digitalen Anwendungen Daten sammeln. Wichtig ist hier, dass man sich über Missstände und Unwohlsein unterhält. Denn erst wenn man über Probleme diskutiert, kann man zu Lösungen kommen. Ein Tipp wäre, sich als Gruppe, sei es als Familie oder als Freundeskreis, über Alternativen zu bisher genutzten Apps zu informieren, beispielsweise zu Messengerdiensten. Dann kann man sich gemeinsam für einen Wechsel von einer Anwendung zur anderen entscheiden. Gerade bei Kindern ist es wichtig, Routinen zum kritischen Umgang mit Medien zu entwickeln. Das geht zum Beispiel mit einer Challenge nach jedem Herunterladen einer neuen App: Wer wählt die datenschutzfreundlichsten Einstellungen?

Dr. Johanna Schäwel,
Universität Hohenheim

Dr. Johanna Schäwel ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Medienpsychologie an der Universität Hohenheim in Stuttgart. Sie forscht zu den Themen Online-Privatheit und Social Media.

Möglichkeiten digitaler Kompetenzbildung im Berufsleben

Beitrag von Alexander Knoth

Pilotprojekt für nationale Bildungsplattform

Innovationen sind der Schlüssel zur Bewältigung großer gesellschaftlicher Herausforderungen und zentral für ein wandlungsfähiges und zugleich leistungsfähiges Bildungssystem. Die digitale Transformation als Innovationschance erfasst dabei alle Sektoren des Bildungswesens und bringt zugleich individuell zugeschnittene Lehr- und Lernformate wie auch neue Kollaborationsmöglichkeiten hervor – das Zusammenwirken von analogem und digitalem Lehren und Lernen erfährt so gänzlich neue Variationsformen, die sich in individuellen Lernpfaden niederschlagen. Ein Ansatz, den digitalen Wandel zu gestalten, besteht in der digitalen Bildungsplattform, die Plattformen und Dienste aus allen Bildungsbereichen bündelt und vernetzt – verfolgt wird dieser Ansatz von der Initiative Digitale Bildung des Bundesministeriums für Bildung und Forschung (BMBF). Künftig soll diese gleichsam als „Hub" fungieren und bundesweit Bildungsplattformen und -angebote über Schnittstellen einbinden, gemeinsame Standards etablieren und in allen Phasen des lebensbegleitenden Lernens den Zugang zu Bildung erleichtern. Der erste Prototyp für eine solche Plattform heißt „Bildungsraum digital" (BIRD) und wurde von einem Verbund entwickelt, der von der Universität Potsdam koordiniert wird und am 1. April 2021 seine Arbeit aufgenommen hat.

Die nationale digitale Bildungsplattform: sektorenübergreifendes Lehren, Lernen und Zusammenarbeiten – ein Werkstattbericht

Das Projekt „Bildungsraum Digital" (BIRD) versteht sich als Prototypenwerkstatt für die technologische Umsetzung sowie die kontinuierliche Verbesserung und Erweiterung einer föderierten Lehr- und Lernlandschaft. Dabei geht es darum, möglichst viele digitale Dienste und Lehr- und Lernmöglichkeiten miteinander zu vernetzen und Übergänge zwischen Systemen und Anwendungen nahtlos digital auszugestalten. Machbarkeitsstudien zu kontext- und szenarioübergreifenden Anwendungsfällen des lebenslangen Lernens sowie die Integration und Einbettung von Dienstleistungsprozessen der Aus- und Weiterbildung entlang der „Learning Journey" von Lernenden oder Lerngruppen stehen dabei im Vordergrund.

Den Zugang zu Lehr/Lernressourcen und -möglichkeiten digital schaffen

BIRD hat das Ziel, digitale Bildungsplattformen zu einer bundesweiten (und europäisch anschlussfähigen) Infrastruktur zu verknüpfen, indem einzelne Komponenten anschlussfähig gemacht werden und zwischen ihnen Interoperabilität hergestellt wird. Somit entsteht ein Ökosystem aus voneinander unabhängigen Bildungsdiensten, das den darin agierenden Nutzer·innen Unterstützung auf ihren Bildungswegen bietet.

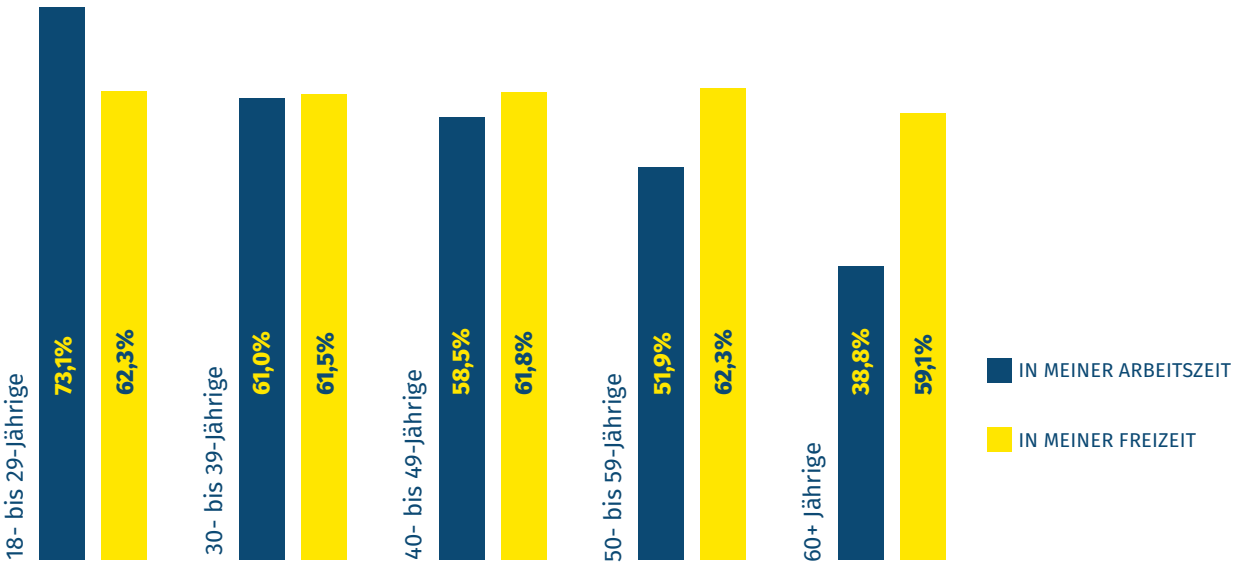
Die Entwicklungen folgen dabei drei Leitprinzipien:

- Menschen vernetzen,
- Inhalte vernetzen und
- E-Learning-Werkzeuge vernetzen.

Das im Projekt verankerte BIRD-Lab bietet in der Funktion eines Inkubators Forschenden und Praktiker·innen eine Umgebung zum Ausprobieren und Implementieren technischer Lösungen der nächsten Generation. Außerdem erfüllt das Lab die Funktion eines Demonstrators, um Lehrenden und Lernenden eine kreative Umgebung zum Erfahren und Ausprobieren neuer Lernsysteme und -prozesse zur Verfügung zu stellen und diese gemeinsam weiterzuentwickeln. Ziel ist es, robuste und erprobte Lösungen aus dem Experimentierlabor in die Plattform zu integrieren.

Das Portal stellt als Kommunikations- und Kollaborationsumgebung den für alle Beteiligten sichtbaren Zugangspunkt zur nationalen digitalen Bildungsplattform dar. Hier sind die Werkzeuge zur Interaktion der Nutzer·innen untereinander und mit dem System zusammengefasst (gemeinsame Lehr-/Lern- und Arbeitsräume, E-Learning-Werkzeuge zur Dokumentation, Zusammenarbeit und Reflexion). Das umfasst sowohl die Bereitstellung von Lerneinheiten, die von anderen Lehrenden wieder genutzt werden können, als auch die Förderung des Austauschs von Lehrenden untereinander. Insbesondere ein solcher kollegialer Austausch (innerhalb einzelner Einrichtungen und darüber hinaus) stellt einen wesentlichen Erfolgsfaktor für die nachhaltige Nutzung einer vernetzten Infrastruktur dar.

Wer würde eine kostenfreie Lernplattform zum Thema Datenschutz in der Techniknutzung nutzen?“



Basis: alle Befragten (n = 2000) Darstellung der Top 2. Angaben in Prozent. Frage Q23: Inwiefern stimmen Sie der folgenden Aussage zu? Ich würde eine kostenfreie Lernplattform zum Thema Datenschutz in der Techniknutzung nutzen (während meiner Arbeitszeit). Ich würde eine kostenfreie Lernplattform zum Thema Datenschutz in der Techniknutzung nutzen (in meiner Freizeit). © Ipsos | Digital Autonomy Hub

Weiterbildung und kollegialen Austausch von Lehrer/-innen fördern

Wie funktioniert BIRD praktisch und welcher Nutzen ergibt sich für die User? Gehen wir von folgendem Szenario aus: Olivia ist Lehrerin der Sekundarstufe II an einer staatlichen Gesamtschule. Covid-19-bedingt findet der Unterricht größtenteils online statt. Olivia fühlt sich methodisch teilweise noch etwas unsicher und möchte daher ihre digitalen Kompetenzen ausbauen. In ihrem Berufsfeld ist es wichtig, auf dem neuesten Stand zu sein, sich stetig fortzubilden und pädagogisch hochwertigen Online-Unterricht anbieten zu können. Über ihre frühere Universität hat sie von BIRD gehört und meldet sich dort mit ihrer Schul-Identität an. Auf Basis ihres Profils und ihrer individuellen Präferenzen findet sie einige für sie hilfreiche Kurse und tritt einem Lehrer·innen-Forum bei. In diesem Forum können sich die Teilnehmer·innen gegenseitig unterstützen und über die neuesten digitalen Inhalte, Innovationen und Fortbildungen austauschen. Ein reibungsloser Übergang zwischen verschiedenen Lernräumen ermöglicht Olivia außerdem die digitale und datensouveräne Umsetzung ihrer Aufgaben sowie eine enge Zusammenarbeit mit anderen Interessengruppen. So ist sie bestens auf ihren Unterricht vorbereitet und kann ihre Schüler·innen beim Lernen in der digitalen Welt optimal begleiten. Auch ihren Kolle·innen empfiehlt sie die Nutzung von BIRD, wodurch die Gemeinschaft der voneinander lernenden Lehrer·innen weiter gestärkt wird und sich der digitale Bildungsraum kontinuierlich weiterentwickeln kann.

Bildungsraum Digital als Werkzeugkasten für Lehrende und Lernende

Bildungsraum Digital trägt zur interaktiven und kooperativen Gestaltung von fachspezifischen Lehr-/Lernszenarien bei, indem die lebenslang Lernenden sowie die sektorenspezifischen und sektorenübergreifenden Angebote miteinander vernetzt werden. BIRD versteht sich selbst als Werkzeugkasten für Lehrende und Lernende, um Dokumentations- und Reflexionsprozesse sowie Prozesse des gemeinsamen Arbeitens digital zu unterstützen. Dafür stehen Foren, Blogs, kollaborative Texteditoren, offene Lernressourcen und viele weitere Funktionen zur Verfügung. Zudem versteht sich BIRD als geschützter Raum, um den kollegialen Austausch zu fördern. Dem ständigen Wandel angepasst soll den Nutzer·innen durch einen einfachen und datensouveränen Zugriff auf unterschiedliche Angebote die Angst vor der (digitalen)

Weiterbildung genommen und selbstbestimmte Handlungen unterstützt werden, ganz nach dem Motto „leave no one behind“.

Ausblick

Im Rahmen der Förderlinie „Initiative Nationale Bildungsplattform“ werden neben dem BIRD-Prototypen noch drei weitere Prototypenprojekte gefördert, die zwar unterschiedliche Vernetzungsansätze verfolgen, jedoch untereinander kompatibel sein werden und sich dahingehend wechselseitig validieren. Ergänzend hinzu kommen noch bis zu 60 weitere Einzelvorhaben, die sich einerseits dem Aufbau lernpfadorientierter Lehr-/Lernangeboten (Ziel-1-Projekte) und andererseits dem Aufbau von Methodenwissen und digitalen Kompetenzen auf Seiten der Lehrenden (Ziel-2-Projekte) widmen. All diesen Projekten steht BIRD als Impulsgeber und Beratungsinstanz zur Verfügung, um mediendidaktische Hilfestellungen sowie Unterstützung bei der Anbindung von digitalen Systemen an BIRD leisten zu können. Konkret bedeutet das, dass der Prototyp BIRD stetig weiterentwickelt und kontinuierlich an den Anforderungen des Bildungswesens wachsen wird.

Alexander Knoth,
Digitalisierungsbeauftragter
DAAD

Alexander Knoth ist Digitalisierungsbeauftragter (CDO) und Leiter des Referats Digitalisierung – S01 beim Deutschen Akademischen Austauschdienst (DAAD). Zuvor arbeitete der passionierte E-Learner an der Universität Potsdam in der Geschlechtersoziologie, als E-Learning Koordinator an der Wirtschafts- und Sozialwissenschaftlichen sowie an der Mathematisch-Naturwissenschaftlichen Fakultät. Am Institut für Informatik und Computational Science beschäftigte er sich mit der Entwicklung von Bildungstechnologien sowie der Komplexität moderner Gesellschaften und Technikgestaltung.

Souveräne Techniknutzung in der nachberuflichen Lebensphase *Interview mit Dr. Janina Stiel*

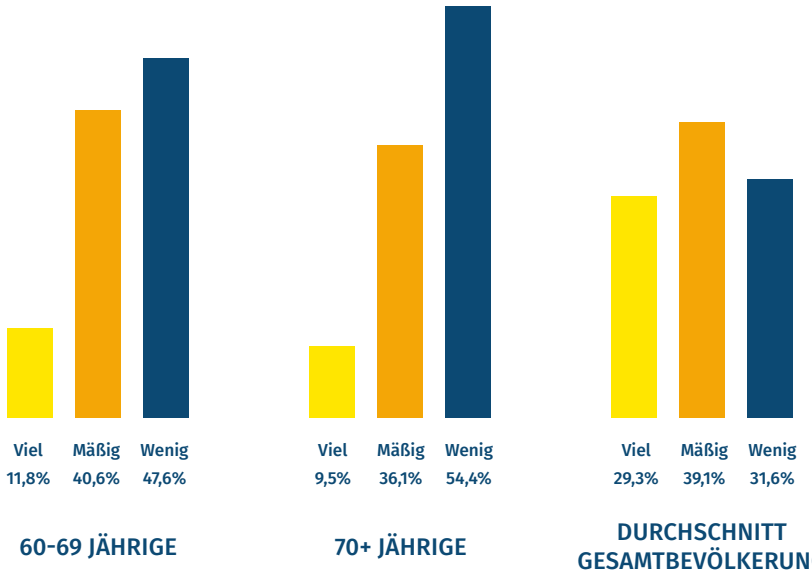
Wie schätzen Sie als Referentin des Projekts „Digitalisierung und Bildung für ältere Menschen" die aktuelle Situation für ältere Menschen in der digitalen Gesellschaft ein?

Dr. Janina Stiel: Das lässt sich so pauschal nicht beantworten, da ältere Menschen sich sehr voneinander unterscheiden. In einer Gesellschaft, in der Kommunikation, Informationsbeschaffung, Einkaufen oder die Inanspruchnahme von Dienstleistungen mehr und mehr im Internet stattfinden, sind diejenigen im Vorteil, die über einen Internetzugang, Geräte sowie Technik- und Medienkompetenz verfügen. Bei der Gruppe der ab 70-Jährigen ist dies aktuell bei der Hälfte der Fall. Bei den älteren Onliner·innen gibt es Anfänger·innen, die nur wenige Funktionen nutzen, Fortgeschrittene, aber auch Expert·innen, die ihr Wissen an andere Ältere weitergeben. Die circa 9 Millionen älteren Offliner·innen sind überwiegend Personen mit geringem Einkommen, geringer formaler Bildung, mit gesundheitlichen Einschränkungen, Hochaltrige, Migrant·innen und Frauen. Hier werden also Menschen, die tendenziell schon stärker sozial exkludiert sind, zusätzlich noch digital abgehängt. Sie profitieren nicht von den Chancen, vermissen diese aber auch kaum, weil sie ihnen gar nicht bewusst sind. Deshalb fühlen sich diese Personen auch nur selten digital abgehängt, sie haben ihre eigenen Strategien entwickelt, ihren Alltag zu bewältigen. Dennoch müssen wir als Gesellschaft etwas gegen die digitale Spaltung innerhalb der älteren Bevölkerung unternehmen und allen, die es möchten, Brücken in die digitale Welt bauen. Allen, die es im Übrigen aus verschiedensten Gründen nicht möchten, sollten ohne Nachteile Wege erhalten bleiben, ihre Angelegenheiten auch analog selbstständig zu bewältigen.

Lernen ältere Menschen anders? Wie wirkt sich dies auf das Erlernen digitaler Kompetenzen aus?

Ältere Menschen haben zum Teil Zweifel an der eigenen Lernfähigkeit, die jedoch unbegründet sind. Die Plastizität des Gehirns ist auch bis ins höchste Lebensalter gegeben, wir können also alle immer dazulernen. Und ja, ältere Menschen lernen anders, wobei auch hier die Unterschiede zwischen den einzelnen Personen erheblich sind und die Veränderungen sowohl Verluste als auch Gewinne bedeuten. Tendenziell kommt es erstens zu kognitiven Veränderungen, wie z. B. einer langsameren Informationsverarbeitung oder einer abnehmenden Kapazität des Arbeitsgedächtnisses. Dafür können Ältere auf mehr Erfahrungswissen aufbauen als Jüngere, was Anschlusslernen begünstigt. Es kommt zweitens zu sensorischen Veränderungen, wie z. B. nachlassende Seh- und Hörfähigkeit. Dies kann über Hilfsmittel und entsprechend angepasste Materialien und Lernumgebungen gut ausgeglichen werden. Drittens verändert sich die Motivation zum Lernen – einer der größten Vorteile. Ältere Menschen lernen tatsächlich eher fürs Leben als für die Schule oder den Beruf. Es geht nicht mehr um äußere Zwänge wie Abschlüsse, Beförderungen oder Zertifikate, es geht allein um die Sache. Motiviertere Lernende können sie kaum haben. Zudem dient das Lernen im Alter nicht allein dem Wissenserwerb, sondern auch dem In-Kontakt-Sein mit anderen, der sozialen Eingebundenheit.
Die Auswirkungen dieser Veränderungen auf das Erlernen digitaler Kompetenzen betreffen vor allem die Gestaltung des Lernsettings. Erfolgreiche Formate sind eine individuelle 1:1-Begleitung oder Kurse in kleinen Gruppen mit mehreren Lernbegleiter·innen, die mit Ruhe und Geduld vorgehen, sich an den Anliegen der Lernenden orientieren, viel wiederholen, Raum für Erfahrungsaustausch

Digitale Aktivität der älteren Generationen



Basis: alle Befragten (n = 2000). Angaben in Prozent.
Frage Q1. Wie oft nutzen Sie folgenden digitale Anwendungen? (Soziale Medien, Suchmaschinen, Nachrichenportale, ...)© Ipsos | Digital Autonomy Hub

und sozialen Kontakt lassen, eine angstfreie, sichere Atmosphäre und am besten auch noch einen Kaffee anbieten. Dies bieten in Deutschland aktuell etwa 400 Gruppen freiwillig engagierter Internethelfer·innen an, die zumeist selbst im Ruhestand sind und genau wissen, worauf es ankommt und welche Ängste bestehen. Sie sind zugleich Rollenmodelle, die zeigen, dass man für den Umgang mit dem Internet nie zu alt ist.

Ältere Menschen sind digital weniger aktiv als jüngere Menschen – dennoch lässt sich auch aus ihrem Leben die Digitalisierung nicht mehr wegdenken. Wie können ältere Menschen zum Erwerb digitaler Kompetenzen motiviert werden?

Ältere Menschen, die das Internet und digitale Anwendungen nicht nutzen, sind keineswegs per se uninteressiert oder müssten nur mal motiviert werden. Vielmehr erscheinen ihnen die Kosten für den erwarteten Nutzen nicht angemessen. Mit Kosten sind die Lebenszeit und der Lernaufwand gemeint, die es erfordert, um die als sehr komplex wahrgenommenen Geräte zu bedienen, sowie das Risiko, im Netz Opfer von Betrügern zu werden oder Daten ungewollt preiszugeben. Auch finanzielle Kosten spielen eine Rolle. Auf der anderen Seite wird nicht erkannt, worin der Nutzen bestehen könnte. Um die Waage so umschlagen zu lassen, dass der erwartete Nutzen die angenommenen Kosten überwiegt und so eine Lernmotivation erzeugt wird, muss jede·r begeistert werden. Das können ganz verschiedene Türöffner sein wie Kontakt halten mit den Enkeln über Messenger oder Videotelefonie, Reisen buchen und sich das Hotel vorab über Street-View ansehen, Discounter-Angebote früher mitbekommen, Mediatheken nutzen, YouTube-Videos über das eigene Hobby oder von alten Lieblingsbands sehen, den Gottesdienst online verfolgen in Zeiten der Pandemie u. v. m.

Abgesehen davon müssen Geräte und Anwendungen durch partizipatives Design tatsächlich nutzerfreundlich werden, müssen in jeder Kommune niedrigschwellige Lerngelegenheiten und konstante Ansprechpersonen da sein für Auswahl, Einrichten und Lernen unterwegs, muss Verbraucherschutz weniger Sache der Verbraucher·innen selbst sein, sondern vielmehr der Hersteller·innen und Anbieter·innen und muss eine Aufklärung über realistische Risiken erfolgen statt Panikmache.

Was braucht es in unserer digitalen Gesellschaft noch, um auch wirklich alle Generationen mitzunehmen und zu beteiligen?

Die digitale Spaltung ist keine Frage der verschiedenen Generationen. Alter spielt in der Tat keine wesentliche Rolle. Die Spaltung verläuft innerhalb der älteren Bevölkerung entlang der auch sonst bekannten Merkmale von sozialer Ungleichheit. Um alle mitzunehmen, bedarf es daher einer Strategie gegen digitale und soziale Ungleichheit in unserem Land. Das wurde ja auch bei den Schüler·innen mit verschiedenem sozialen Hintergrund im Homeschooling offensichtlich. Maßnahmen, um die Teilhabe auch für aktuell abgehängte Personen zu sichern, wären z. B. die Verfügbarkeit von schnellem Internet in allen Wohnformen älterer Menschen und in allen öffentlichen Einrichtungen, Übernahme der Kosten für einen Internetanschluss und ein Gerät für Menschen mit geringem Einkommen über sozialrechtliche Hilfe im

SGB XII, Lern- und Erfahrungsorte zum Sehen und Ausprobieren von Technologien in jeder Kommune, geragogisch qualifizierte Technikbegleiter·innen in jeder Kommune, mehr Informationen und Lernformate in den öffentlich-rechtlichen Medien, die die Offliner·innen überdurchschnittlich häufig nutzen und eine Sensibilisierung der Hersteller·innen und Designer·innen für die tatsächlichen Bedarfe ihrer größten Kundengruppe. Außerdem brauchen Berufsgruppen, die mit älteren Menschen interagieren, mehr digitale Kompetenzen in ihrer Aus- und Weiterbildung.

Futuristisch gedacht: Wie sieht digitale Bildung und Kompetenzerwerb für ältere Menschen Ihrer Meinung nach in zehn bis zwanzig Jahren aus?

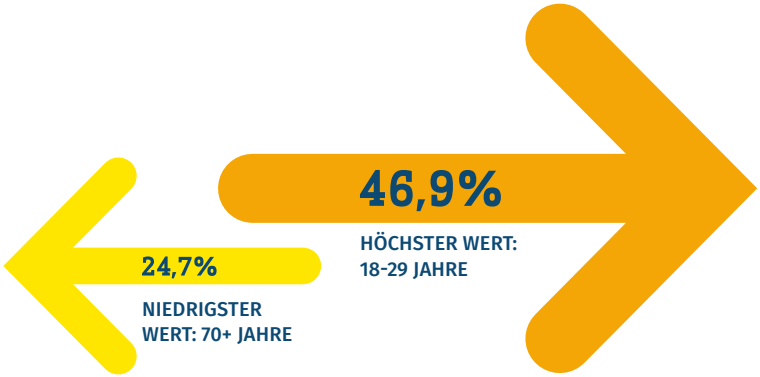
Das ist eine spannende Frage. Ich gehe davon aus, dass digitale Bildung in der nachberuflichen Lebensphase ein Handlungsfeld bleiben wird und der Bedarf mit der Alterung der Gesellschaft und der fortschreitenden Digitalisierung sogar wächst. Man könnte vermuten, dass die Bildungsinhalte sich dann weniger auf den ersten Einstieg ins Netz beziehen, weil nachrückende Kohorten den in der Regel schon vollzogen haben. Jedoch schreitet ja auch die Technologieentwicklung immer schneller voran und unser Wissen veraltet schneller, und so kann die Wissenslücke auch ebenso groß oder größer sein als jetzt, nur auf höherem Niveau. Ich vermute eine Ausweitung der Technikberatung und -begleitung noch stärker auf Felder außerhalb von IKT, also auch mehr Smart Home, Gesundheitstechnologien, Robotik, Mobilitätslösungen.

Ich hoffe, dass wir bis dahin reguläre Studien- und Ausbildungscurricula haben, die Fachkräfte an der Schnittstelle von technologischem Wissen und Geragogik hervorbringen. Und dass die digitale Bildung im Alter bis dahin einer bundesweiten Bildungsstrategie folgt, die auch hauptamtlich Lehrende vorsieht und die Verantwortung nicht hauptsächlich auf den Schultern freiwillig Engagierter lastet.

Dr. Janina Stiel,
BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e.V.
© BAGSO – Herby Sachs

Dr. Janina Stiel leitet die Servicestelle „Digitalisierung und Bildung für ältere Menschen“ bei der BAGSO, gefördert vom BMFSFJ. Sie ist seit zwölf Jahren im Bereich Geragogik tätig, Autorin mehrerer Bücher und Ko-Autorin einer Expertise für den Achten Altersbericht der Bundesregierung „Alter und Digitalisierung“. Ihre Promotion in Sozialer Gerontologie hat sie 2021 an der TU Dortmund abgeschlossen.

Junge Menschen finden Chatbots tendenziell hilfreich, um Datenschutzerklärungen zu verstehen, ältere eher nicht.



Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q26a: Stellen Sie sich vor, Sie haben die Möglichkeit, einen interaktiven Chatbot zur Datenschutzerklärung eines Geräts/einer App zu befragen. Können Sie dadurch die Datenschutzerklärung besser verstehen? © Ipsos | Digital Autonomy Hub

Innovative Einblicke: ASSISTENZ- UND DIALOGFORMATE

Virtuelle Dialogformate wie Chatbots und virtuelle Empfehlungssysteme eröffnen neue Möglichkeiten für den unabhängigen, selbstgesteuerten Erkenntnisgewinn und damit für die Steigerung der digitalen Souveränität. Nutzer·innenzentrierte Assistenz- und Dialogformate können komplexe Entscheidungssituationen zur eigenen Datenweitergabe oder zur bestmöglichen Nutzung von Anwendungen im Sinne der Nutzer·innen nachvollziehbarer und niedrigschwelliger machen. In der selbstgesteuerten Auseinandersetzung mit Sachverhalten gewinnen Nutzer·innen an Wirkmacht und erfahren Unterstützung.

PANDERAM – *Privatsphären-Analyse und nutzerspezifische Datenschutzempfehlungen für Apps und Mobilgeräte*

PANDERAM

Webseite
https://www.interaktive-technologien.de/projekte/panderam

Vorhaben
Niedrigschwelliger Zugang zu Datenschutz und -sicherheit auf dem eigenen Smartphone soll z. B. über eine App angeboten werden. Die Analysen von Apps und des Android-Betriebssystems werden automatisiert ausgeführt. Die Ergebnisse resultieren in entsprechenden Scores und konkreten Handlungsempfehlungen.

Zielgruppe
Smartphone-Nutzer·innen mit Interesse am Schutz ihrer Daten. Dabei sollen verschiedene Verhaltensstufen differenziert und adressiert werden.

Assistenten + Dialogformate im Projekt
Die Einschätzungen werden in verständlichen Dialogen erläutert, die Handlungsempfehlungen passend zur Verhaltensstufe gegeben und Nutzer·innen dadurch nicht über- oder unterfordert. Die Darstellung als Scores soll motivieren, Handlungsempfehlungen, wie bspw. die Installation von vorgeschlagenen App-Alternativen, umzusetzen.

Partner
Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Institut für Technik & Journalismus e. V., secuvera GmbH, Technische Universität Berlin – DAI Labor, Technische Universität Chemnitz

DigS-Gov – *Digitale Souveränität im E-Government*

Webseite https://jil.sh/projekte/digs-gov/

Vorhaben Im Projekt werden fünf Demonstratoren in den Bereichen Visualisierung und Micro-Learning (Information), Simulation und Gamification (Interaktion) sowie Entscheidung und Feedback (Transaktion) für E-Government-Dienste entwickelt. Diese können von öffentlichen Verwaltungen vor, während oder nach der Nutzung ihrer Angebote eingesetzt werden.

Zielgruppe Nutzer·innen von E-Government-Services

Assistenten + Dialogformate im Projekt Die menschzentrierten Informations- und Interaktionsangebote von DigS-Gov sprechen breite Teile der Bevölkerung bei Kontakten mit öffentlichen Verwaltungen an. Hierdurch fördern wir digitale Kompetenzen.

Partner Institut für Multimediale und Interaktive Systeme (IMIS) der Universität zu Lübeck, Ethical Innovation Hub der Universität zu Lübeck, Hansestadt Lübeck, MACH AG, Nucleon e. V.

VICON – *Virtueller Consent-Assistant*

Webseite https://vicon-projekt.org/

Vorhaben Ziel von ViCon ist es, Bürger·innen zum selbstbestimmten Umgang mit Einwilligungen in die Verarbeitung von personenbezogenen Gesundheitsdaten zu befähigen. Dabei soll die Informiertheit der Bürger·innen gesteigert, ihre Wertvorstellungen ernst genommen und ihr Vertrauen gesteigert werden.

Zielgruppe Bürger·innen und Patient·innen, die in die Verarbeitung von personenbezogenen Gesundheitsdaten einwilligen

Assistenten + Dialogformate im Projekt ViCon stellt die Informiertheit der Patient·innen abhängig vom Informationsstand anhand von personalisierten adaptiven Lern- und Informationsinhalten sicher. Im Fokus stehen der datensouveräne Umgang und das gesteigerte Vertrauen. Zudem ermöglicht die Implementierung eines Einwilligungsmodells die präzisere Abbildung des Willens der Patient·innen.

Partner FernUniversität in Hagen, Fraunhofer-Gesellschaft München (Fraunhofer ISST Dortmund, Fraunhofer IMW Leipzig), Kairos GmbH Bochum, Universität zu Köln

4/ TECHNIK-GESTALTUNG

Individuelle digitale Souveränität braucht innovative Interaktionsformen, die die Bedarfe, Kompetenzen und die Ermächtigung der Nutzer·innen ins Zentrum stellen. Ein wichtiges Moment ist die Integration der in den vorherigen Kapiteln besprochenen Prinzipien zum Schutz der Rechte der Nutzenden in den Innovationsprozess. Auch die genannten Aspekte zur Unterstützung beim Selbstdatenschutz sollten im Innovationsprozess berücksichtigt werden. Im Kapitel „Technologieentwicklung und Innovation“ wird deshalb beleuchtet, wie Wissenschaft, Technik, Wirtschaft und Nutzer·innen interagieren können, um die digitale Souveränität zu erhöhen.

Chancen der menschenzentrierten Technikforschung *Interview mit Prof. Dr. Claudia Müller-Birn*

In der aktuellen Umfrage des Digital Autonomy Hubs haben 45 % der Befragten angegeben, sich mit dem Schutz ihrer persönlichen Daten in der Nutzung von digitalen Geräten und Anwendungen überfordert zu fühlen. In der jüngsten Altersgruppe (18–30 Jahre), die Gruppe der Vielnutzer·innen, sind es sogar 60 %. Welche Ansätze gibt es in der aktuellen Forschung und speziell im Human-Centered-Computing, um diese wahrgenommene Überforderung zu adressieren?

Prof. Dr. Claudia Müller-Birn: Studien haben gezeigt, dass Datenschutzerklärungen für die durchschnittliche Leserschaft meist zu lang und zu schwer verständlich sind. Entscheidungen bezüglich des Datenschutzes werden von Personen häufig schnell und intuitiv getroffen. Zudem gibt es bei den gängigen Datenschutzoptionen meist keine wirkliche Wahl bzw. Entscheidungsmöglichkeit. Diese Probleme sind bekannt und es gibt bereits vielfältige Vorschläge aus der Forschung, diesen Herausforderungen zu begegnen. Lassen Sie mich einige Ansätze beispielhaft herausgreifen.

Ein naheliegender Weg der Vereinfachung ist, neben der verbesserten Strukturierung von Datenschutzerklärungen, die Verwendung von Bildsymbolen. Dieser Ansatz ist bereits in der DSGVO vorgesehen.

Darüber hinaus existieren unterschiedliche Ansätze dafür, Datenschutzerklärungen durch Visualisierungen verständlicher aufzubereiten. Die Datenschutzerklärungen werden dabei maschinell mit Methoden des *Natural Language Processing* analysiert und visualisiert. Ein Beispiel dafür ist das Projekt Polisis.
Andere Lösungen ermöglichen es den Nutzer·innen, ihre Datenschut-

zeinstellungen besser mit Hilfe sogenannter *Personal Information Management Systeme* (PIMS) zu überwachen. Die Idee dahinter: Indem die Kontrollrechte einer Person technisch unterstützt werden, wird auch der individuelle Datenschutz verbessert. Ein Vorschlag diesbezüglich wurde bereits im Jahr 2002 von Lorrie Cranor mit der *Plattform for Privacy Preferences* (P3P) erarbeitet. Diese Plattform sollte Personen dabei helfen, schnell einen Überblick darüber zu erhalten, was mit ihren personenbezogenen Daten geschieht, die beim Besuch einer Webseite anfallen. P3P wurde vom *WWW Consortium* (W3C) im Jahr 2002 als Standard empfohlen, konnte sich in der Industrie aber leider nicht durchsetzen.

Als Grund für die individuelle Nichtumsetzung von Datenschutz wurde vor allem die schwere Auffindbarkeit von Einstellungsmöglichkeiten genannt. Wie können wir die Erkenntnisse aus der Forschung in die Anwendung bringen, um das Handling auch für nicht technikaffine Nutzer·innen zu erleichtern?

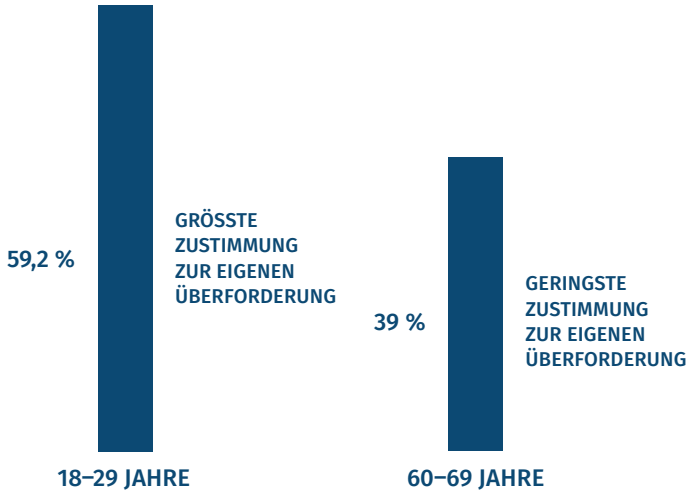
In der Tat: Datenschutzerklärungen oder -einstellungen, wie im Fall von Cookie-Bannern, bieten Nutzenden häufig keine oder nur umständliche Möglichkeiten, diese auf ihre Datenschutzbedürfnisse anzupassen. Das Ziel beim Design von User-Interfaces für Datenschutzerklärungen oder -einstellungen sollte daher sein, sie möglichst einfach zu gestalten. Das passiert im Grunde genommen bereits heute: Wir alle kennen Cookie-Banner, bei denen wir einen großen grünen und einen kleinen grauen Button sehen. Diese Form der Gestaltung macht es uns scheinbar leichter, eine Auswahl zu treffen: denn fast automatisch wählen wir den grünen Button. Diese Auswahl führt aber genau dazu, dass wir nun alle personenbezogenen Daten mit dem Unternehmen teilen, was wir gar nicht wollten. Die hier beschriebene Form der Gestaltung verwendet sogenannte ‚Dark Patterns'. Solche Gestaltungsmuster machen es sich zunutze, dass wir die meisten unserer täglichen Entscheidungen instinktiv und unbewusst treffen, beispielsweise indem wir die grüne und nicht die kleine graue Schaltfläche auswählen. Die Frage ist also: Wie können wir Datenschutzerklärungen oder -einstellungen verständlicher und im Sinne der Wahrung der Privatsphäre von Nutzenden gestalten, ohne auf solche manipulativen Designtechniken zurückzugreifen? Mögliche Ansätze (z. B. Bildsymbole, Visualisierung, PIMS) habe ich bereits genannt, aber diese Ansätze werden in der Breite von Unternehmen nur wenig bis gar nicht berücksichtigt.

Wenn Sie den aktuellen akademischen Diskurs betrachten, gibt es innovative Neuerungen in der Mensch-Computer-Interaktion? Wo gehen wir voraussichtlich in den nächsten Jahren über Bekanntes hinaus?

Innovative Datenschutzlösungen gibt es in unterschiedlichen Forschungs- und Anwendungsgebieten, beispielsweise im Bereich IoT (z. B. Smarthome-Geräte oder Wearables), da hier häufig keine visuellen Anzeigen verfügbar sind und andere Formen der Informationsvermittlung genutzt werden müssen.

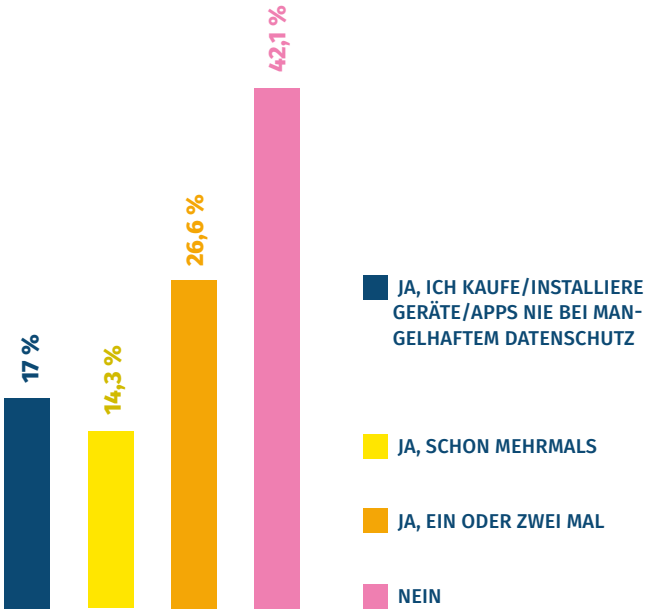
Ein weiteres Anwendungsgebiet ist der Bereich des Maschinellen Lernens. In diesem Bereich existiert zwar eine Reihe von mathematischen Ansätzen für den Datenschutz, aber deren Anwendbarkeit konnte bisher nur in wenigen praktischen Beispielen geprüft werden. Auch im Bereich des UX-Designs wird nutzer·innenorientiert erforscht, wie aufdringliche Push-Benachrichtigungen, Genehmigungsanfragen oder Tracking durch Dritte nachvollziehbarer gestaltet werden können. Innovationen lassen sich ebenfalls im Interaktionsdesign finden, beispielsweise durch den Einsatz von *Conversational Interfaces*. Hier liegt eine große Herausforderung im Bereich der Informationskomplexität. Darüber hinaus werden auch verstärkt Ansätze erforscht, Personen nicht nur genauer über ihre Wahlmöglichkeiten zu informieren, sondern ihnen eine wirkliche Auswahl in Bezug auf ihre Datenweitergabe

Besonders jüngere Menschen fühlen sich beim Datenschutz überfordert.



Basis: alle Befragten (n = 2000). Darstellung der Top 2 und Bottom 2. Angaben in Prozent. Frage Q17: Ich fühle mich im Alltag mit dem Schutz meiner persönlichen Daten bei der Nutzung digitaler Geräte und Anwendungen überfordert. © Ipsos | Digital Autonomy Hub

Ein Teil der Befragten entscheidet sich bei mangelhaftem Datenschutz gegen die Nutzung eines Geräts/einer App.



Basis: alle Befragten (n = 2000) Angaben in Prozent. Frage Q13: Kam es schon mal vor, dass Sie ein Gerät oder eine App kaufen bzw. installieren wollten, sich dann aber in Anbetracht von mangelndem Datenschutz dagegen entschieden? © Ipsos | Digital Autonomy Hub

oder Datenschutzeinstellungen zu eröffnen.

Gibt es Risiken für die digitale Mündigkeit von Nutzer·innen in diesen Innovationen? Wie schätzen Sie diese ein?

Das Risiko liegt meines Erachtens weniger in der Nutzung solcher Ansätze zur Realisierung des Datenschutzes, sondern in der öffentlichen Wahrnehmung dieses Themas. Datenschutz wird häufig als Verhinderer von Innovation begriffen. Dabei wird jedoch außer Acht gelassen, dass die informationelle Selbstbestimmung ein Grundrecht ist und daher im Datenschutz Innovationspotenzial liegt. Ein Risiko für die digitale Mündigkeit von Nutzer·innen besteht also darin, dass der gesellschaftliche Wert des Datenschutzes eine weitere Abwertung erfährt. Daher ist ein wesentliches Anliegen meiner Forschung, Personen dabei zu unterstützen, regelmäßig und bewusst über Datenschutzfragen und -entscheidungen nachzudenken und zu reflektieren.

Sie koordinieren das Projekt WerteRadar, in dem prototypische Lösungen zur Mündigkeit bei der Datenweitergabe im klinischen Kontext entwickelt werden. Können Sie uns einen kurzen Einblick geben?

In unserer Forschung setzen wir uns mit der Frage auseinander, welche Auswirkungen unsere Entscheidungen als Gestalter·innen und Entwickler·innen beim Design einer Technologie auf die unterschiedlichen Interessengruppen haben, die vom Einsatz der Software betroffen sind. Es ist uns ein Anliegen, dass Nutzer·innen einer Technologie die potenziellen Konsequenzen, in diesem Fall die Risiken der Datenweitergabe und die damit verbundenen Optionen, verstehen, um somit eine fundierte und wohlinformierte Entscheidung treffen zu können. Im Projekt WerteRadar erforschen wir diese Frage im medizinischen Kontext mit einem interdisziplinären Verbund aus Expert·innen der Mensch-Maschine-Interaktion, Datensicherheit, Medienpädagogik und Medizin.

Prof. Dr. Claudia Müller-Birn, Freie Universität Berlin, Institut für Informatik, Forschungsgruppe Human-Centered Computing
© Frank Woelffing

Prof. Müller-Birn forscht in den Bereichen Collaborative Computing und Mensch-Maschine-Interaktion. Ihr Fokus liegt dabei auf sozial verantwortlichen Technologien mit einem aktuellen Schwerpunkt auf dem Maschinellen Lernen mit Bezug zu Fragen der Privatsphäre, der Reflexion und der Erklärbarkeit.

Verantwortung von und ethische Grundsätze für Entwickler·innen *Interview mit Alexander von Gernler*

In der Umfrage des Digital Autonomy Hubs stößt die Idee, dass Entwickler·innen verpflichtende Kurse zu Transparenz, Privatheit und Ethik belegen müssen auf hohe Zustimmung. 75 % der Befragten sprechen sich dafür aus. Kommen diese Themen im Berufsalltag überhaupt vor?

Alexander von Gernler: Mir selbst sind im eigenen Berufsalltag in über 15 Jahren nahezu keine solchen Angebote begegnet. Ich glaube, dass derartige Kurse bei Firmen auch immer in Konkurrenz zu anderen Fortbildungen stehen, die für Arbeitgeber·innen und Angestellte im Vergleich einen greifbareren und konkreteren Nutzen verheißen, wie etwa Zeit- und Stressmanagement, Konfliktmanagement, Rhetorik und andere Seminare mit hohem Praxisbezug. Wenn Leute sich mit diesen Themen beschäftigen, dann geschieht das nach meinem Eindruck eher aus eigener Motivation heraus und in ihrer Freizeit – aus den genannten Gründen. Diese Leute besuchen dann etwa Veranstaltungen von Vereinen, die technisches Interesse mit bürgerrechtlichem Engagement verbinden, oder organisieren sich selbst in solchen Initiativen.

Wo müssen Entwickler·innen im Entwicklungsprozess ethisch relevante Entscheidungen treffen? Gibt es dafür konkrete Beispiele?

Frei nach Joseph Weizenbaum würde ich empfehlen, die Situation immer vom Ende her zu denken: Ich kann mich also in der Ausübung meiner Kunst ganz toll mit Bilderkennung in neuronalen Netzen beschäftigen, muss aber wissen, dass meine Technologie dann auch in der kompletten Kameraerfassung von Innenstädten oder in der Steuerung von Lenkraketen eingesetzt werden kann. Im Fall von Cambridge Analytica haben Leute sich Gedanken gemacht, wie man aus einer Kombination relativ trivialer Facebook-Likes („Ich mag Elton John“) Rückschlüsse auf Alter, Geschlecht, sexuelle Orientierung und politische Einstellung treffen kann. In der Verlängerung hat diese Technologie aber bedeutet, dass damit zumindest versucht wurde, Wahlen zu beeinflussen. Es beginnt schon bei ganz einfachen Fragen wie etwa der Datensparsamkeit, die heute ja nach der Datenschutz-Grundverordnung auch geboten ist: Muss ich denn in einem Formular bestimmte Daten wirklich abfragen oder geht es auch mit weniger?

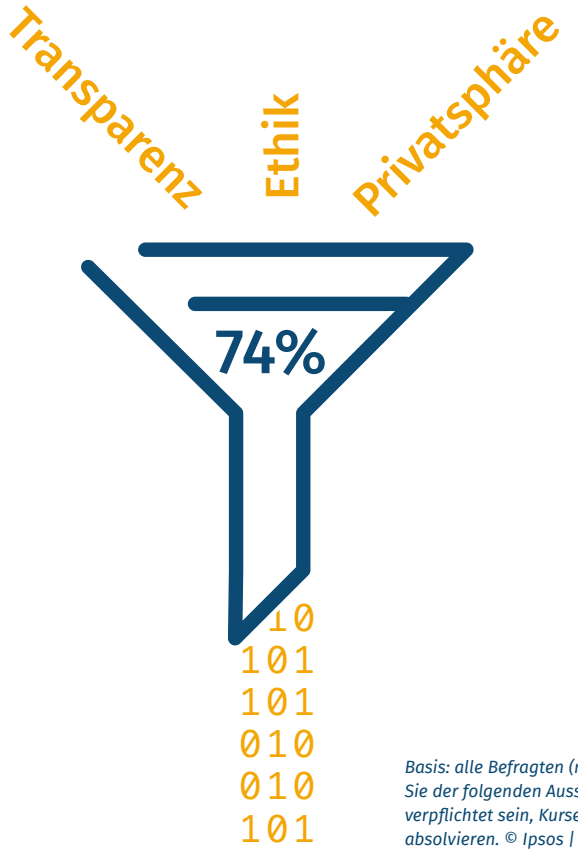
Ist es in der Praxis üblich, dass Konsequenzen der eigenen Innovation schon im Entwicklungsprozess kritisch hinterfragt werden?

Aus meiner praktischen Erfahrung gibt es gerade in der deutschsprachigen Community eine hohe Bereitschaft, das eigene Tun zu hinterfragen. Dort spielen Einflüsse wie die Hackerethik des Chaos Computer Clubs, die Stimmen von Datenschutz- und Bürgerrechtsinitiativen eine Rolle, aber historisch betrachtet auch die Volkszählung 1984 oder wegweisende Urteile des Bundesverfassungsgerichts, das ja das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf die Integrität informationsverarbeitender Systeme geschaffen hat.

Das schlägt sich dann auch im Handeln von Angestellten nieder, die gegen bestimmte Projekte protestieren, die aus ihrer Sicht zu nahe am Militär oder am Geheimdienst operieren, oder hinterfragen, ob man Aufträge aus bestimmten arabischen Staaten annehmen sollte, wo Menschenrechte missachtet werden.

In Debatten rund um Digitalisierung und Technik sprechen wir oft über Verantwortungsvertei-

74% der Befragten wollen Entwickler·innen dazu verpflichten, an Weiterbildungen zu Transparenz, Privatsphäre und Ethik teilzunehmen



Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q19: Inwiefern stimmen Sie der folgenden Aussage zu? Entwickler·innen von digitalen Technologien sollten verpflichtet sein, Kurse und Weiterbildungen zu Transparenz, Privatsphäre und Ethik zu absolvieren. © Ipsos | Digital Autonomy Hub

lung und ethische Grundsätze für den Einsatz neuer Technologien, zum Beispiel Künstlicher Intelligenz. Seltener werden dabei die Entwickler·innen selbst betrachtet oder in die Diskussion eingebunden. Warum ist das so und ist das problematisch?

Es ist richtig, dass die Diskussion über die Folgen von Technik eher nicht in technischen Fachzeitschriften oder anderen Fachmedien erfolgt, denn da geht es meistens nur um das „Wie". Wenn über Technikfolgen, Ethik und Verantwortung geredet wird, dann passiert das aber inzwischen auch in den Feuilletons der großen deutschsprachigen Tageszeitungen. Für mich ist das ein Signal, dass die Debatte eine hohe gesellschaftliche Relevanz erreicht hat – einfach deswegen, weil die Informatik in den letzten zwei Jahrzehnten global und fundamental die Art und Weise verändert hat, wie wir denken, leben, kommunizieren und arbeiten. Die Debatte wird im Moment hauptsächlich von Philosoph·innen, Soziolog·innen und Feuilletonist·innen geführt. Aus den Reihen der Techniktreibenden sind da die Stimmen eher noch dünn. Das finde ich zunächst einmal sehr verständlich, weil die Beschäftigung mit Technik natürlich sehr zeitintensiv ist und Kommunikation nicht jedem Menschen liegt. Die Virologie macht uns aber in der Pandemie gerade vor, welchen Wert es hat, auch direkt in den Dialog mit der Gesellschaft zu gehen.

Welche Änderungen bräuchten wir in der aktuellen Situation, um die negativen gesellschaftlichen Folgen von Technologieentwicklung und Innovation besser zu navigieren?

Wir erleben seit geraumer Zeit schon eine Transition von Systemen, die wir als Benutzende komplett unter Kontrolle haben und überblicken können, hin zu

Systemen, deren Komplexität selbst für Expert·innen nicht mehr als einzelne Person begreifbar ist und die sich zunehmend unserer Kontrolle entziehen. Ausgangspunkt waren die immer reichhaltigeren Endbenutzersysteme, bei denen schon Betriebssystemkern und Browser eine enorme Komplexität aufwiesen. Da war aber noch alles lokal. Jetzt sehen wir Trends, die das Ganze noch weit übersteigen. Die Cloud schafft den Aspekt der lokalen Kontrolle ab und die neuronalen Verfahren in der KI stellen uns vor die Frage der Nachvollziehbarkeit von maschinellen Entscheidungen. Wir sind als menschliche Gesellschaft global leider immer noch in der Rezeptionsphase und werden das wegen der hohen Innovationsdichte und -geschwindigkeit auch noch lange bleiben. Wichtig ist aber, dass wir die Debatte über die Technologien am Leben erhalten und uns vor allem darauf besinnen, dass die Innovationen den Menschen dienen sollen, und nicht umgekehrt. Das Primat der Gesellschaft und der Politik ist also entscheidend. Das bedeutet aber, dass wir selbst erst einmal positiv formulieren müssen, wie wir leben wollen. Schaffen wir das nicht, wird neue Technik uns in unserer Wahrnehmung immer „zustoßen“.

Alexander von Gernler,
Vizepräsident der Gesellschaft
für Informatik; Research and
Innovation, genua GmbH
© Nicolas Wefers

Alexander von Gernler beschäftigt sich beruflich mit den technologischen Fortschritten im Bereich IT-Sicherheit und stößt in diesem Themenfeld regelmäßig Forschungsprojekte und Inkubatoren an. Was ihn aber seit Beginn seines Informatikstudiums schon beschäftigt hat, ist die Frage, wie Informatik die Gesellschaft verändert.

79 % der Befragten finden, dass es eine Datenschutz-Ampel geben sollte, die anzeigt, wie datenschutzfreundlich eine Anwendung ist.[II]

[II] Basis: Alle Befragten (n = 2000). Darstellung der Top 2. Frage Q22: Inwiefern stimmen Sie den folgenden Aussagen zu? Es braucht ein einfaches Qualitätssiegel (z.B. eine Datenschutz-Ampel), das zeigt, wie datenschutzfreundlich eine Anwendung ist.
© Ipsos | Digital Autonomy Hub

Innovative Einblicke: INTERAKTIVE VISUALISIERUNG

Die Zusammenhänge zwischen der Nutzung digitaler Technologien und Geräte und den von ihnen erhobenen Daten sind selbst für Expert·innen schwer zu erfassen. Interaktive Visualisierungen können komplexe Informationen begreifbar machen. Nutzer·innen treten in den direkten Austausch mit den sonst unsichtbar bleibenden, wachsenden Datenmengen, die auch im Alltag entstehen, verarbeitet und weitergegeben werden. Zusammenhänge werden so buchstäblich sichtbar und dadurch leichter verständlich.

SIMPORT – *Souveränes und Intuitives Management personenbezogener Ortsinformationen*

SIMPORT

Webseite **https://simport.net/**

Vorhaben SIMPORT entwickelt Ansätze, Visualisierungen und Softwaremodule für das souveräne Management der eigenen Ortsinformationen auf mobilen Endgeräten. Dabei entsteht frei verfügbare Software, die mögliche Rückschlüsse aus diesen Ortsinformationen verständlich visualisieren und Nutzer·innen mehr Kontrolle über deren Weitergabe gibt.

Zielgruppe Das Projekt wendet sich sowohl an Bürger·innen als auch an Anbieter·innen von ortsbasierten Diensten sowie an Software-Entwickler·innen.

Interaktive Visualisierung im Projekt Im Projekt wird u. a. ein interaktives Lerntool entwickelt, das die Zusammenhänge zwischen der Weitergabe eigener Ortsinformationen und den daraus resultierenden potenziellen Gefahren visualisiert. Auch neuartige Bedienelemente werden entstehen, z. B. zur besseren Kontrolle der Informationsweitergabe.

Partner FH Münster, HERE Deutschland GmbH Berlin, Reedu GmbH & Co KG Münster, Technische Universität Berlin, Westfälische Wilhelms-Universität Münster

InviDas – *Interaktive, visuelle Datenräume zur souveränen, datenschutzrechtlichen Entscheidungsfindung*

Webseite https://invidas.gi.de/

Vorhaben In einem virtuellen Dashboard sind Fitnesstracker und andere Smart Wearables vergleichbar: Nutzer·innen können sehen, welche Daten bei der Nutzung mit wem und zu welchem Zweck ausgetauscht werden, sie können ihr eigenes Datenprofil erfassen und in virtuellen Escape-Rooms ihre Kompetenzen spielerisch trainieren.

Zielgruppe (potenzielle) Nutzer·innen von Fitnesstrackern, Hersteller·innen von Smart Wearables

Interaktive Visualisierung im Projekt Durch interaktive Infografiken und Gamification werden textuelle Datenschutzerklärungen erfahrbar. Damit geht InviDas über bisherige Ansätze zur Bebilderung von Datenschutzerklärungen hinaus

Partner Gesellschaft für Informatik e.V., Stiftung Digitale Chancen, Garmin Würzburg GmbH, RWTH Aachen, Universität Bremen und Otto-Friedrich-Universität Bamberg

USABLESEC@HOME – *Erfahrbarer Datenschutz und IT-Sicherheit in Smarthome-Anwendungen*

Webseite https://usablesecathome.de/

Vorhaben Es entsteht eine auf Augmented Reality (AR) basierende Simulation und Visualisierung von Datenflüssen in einem Smarthome-System. Diese Visualisierung dient dem besseren Verständnis des Datenschutzes und der Informationssicherheit in einem Smarthome.

Zielgruppe Alle Nutzer·innen, die bei sich zu Hause bereits ein Smarthome-System einsetzen oder planen, ein solches zu installieren

Interaktive Visualisierung im Projekt Datenflüsse in einem Smarthome werden Nutzer·innen mittels AR transparent gemacht. Dies geschieht über eine Smartphone-App oder Mixed-Reality-Headsets. Hierdurch erhalten Nutzer·innen ein besseres Verständnis, wohin datenschutz- und sicherheitskritische Daten fließen und wie diese gesichert sind.

Partner Universität Bremen, neusta mobile solutions GmbH, Ruhr-Universität Bochum, Certavo GmbH

Die Wirtschaftlichkeit individueller digitaler Souveränität *Interview mit Dr. Marija Radić*

Laut unserer Umfrage haben nur 42 % der Befragten den Eindruck, dass es ausreichend datenschutzfreundliche Alternativen bei Anwendungen und Geräten gibt. Deckt sich das mit Ihrer Einschätzung oder sind uns die Alternativen einfach nicht präsent?

Dr. Marija Radić: Unsere bisherigen Forschungserkenntnisse zeigen, dass Bürger·innen sehr unterschiedliche Bedürfnisse im Hinblick auf den Schutz ihrer Daten haben. Es hat sich auch gezeigt, dass die Bedeutung und der Umgang mit dem Thema Datenschutz sich je nach Markt unterscheiden. Dennoch deckt sich die Statistik auch mit unserer Forschung: Aktuell ist Datenschutz nur für wenige Unternehmen ein Thema, das über die Einhaltung gesetzlicher Regularien hinausgeht. Wir bevorzugen daher den Begriff der Datensouveränität. Er markiert, dass es um mehr geht – nämlich darum, Anwender·innen darin zu befähigen, autonom Entscheidungen zum Umgang mit ihren Daten zu treffen. Dass die befragten Nutzer·innen keine datenschutzfreundlichen Alternativen wahrnehmen, liegt nicht zuletzt daran, dass Unternehmen Datensouveränität noch nicht als strategisches Thema erkannt haben.

Was bewegt Menschen dazu, datenschutzunfreundliche Geräte oder Anwendungen zu verwenden? Wo sehen Sie die größten Hürden für Selbstdatenschutz bei der Kauf- bzw. Installationsentscheidung?

Die Gründe hierfür sind vielfältig. So ist zum Beispiel auf Ebene der Nutzer·innen festzustellen, dass unzureichender Datenschutz in der Regel kein K.O.-Argument bei der Anbieterwahl ist – insbesondere dann nicht, wenn die angebotene Dienstleistung sehr gut oder mit niedrigen Kosten verbunden ist. Zudem zeigt sich, dass geltende Datenschutzbestimmungen nicht immer umfassend und transparent kommuniziert werden, es den Nutzer·innen aber auch häufig an Datenkompetenz fehlt,

Über die Hälfte der älteren Menschen würde gar nichts für Datenschutz bei einer App ausgeben. Im Schnitt würden sie unter 4 € zahlen, während die 18- bis 29-Jährigen durchschnittlich 9,10 € zahlen würden.

Basis: alle Befragten (n = 2000). Angaben als Mittelwert (enthält 0 €). Frage Q24: Stellen Sie sich vor, Sie können bei einer von Ihnen häufig genutzten Anwendung (z. B. Nachrichtendienst, soziales Medium, Spiele-App) einen bestimmten Geldbetrag zahlen und anschließend Ihre Daten selbst verwalten. Wie viel wären Sie bereit, dafür einmalig auszugeben? © Ipsos | Digital Autonomy Hub

was die Auswahl datenschutzfreundlicher Angebote erschwert. Die Probleme liegen aber auch marktseitig. Denn häufig gibt es schlichtweg keinen alternativen Anbieter, der sowohl einen besseren Datenschutz als auch eine mindestens gleichwertige Leistung bietet. Unsere aktuellen Forschungen zeigen, dass das Spannungsfeld zwischen Datenökonomie und -souveränität sehr komplex ist, weil sowohl Marktwirtschaft als auch Regulatorik eine Rolle spielen. Im Positionspapier „Data Sovereignty and Data Economy — Two Repulsive Forces?“ haben wir mögliche Lösungsansätze dazu aufgezeigt.

Wie sieht das auf der Seite der Technologieanbieter aus? Welche Anreize haben Unternehmen, auf Datenschutz zu setzen? Lässt sich ein positiver Effekt feststellen, wenn sie es tun? Oder sind datenbasierte Geschäftsmodelle gar unvereinbar mit digitaler Souveränität?

Datenbasierte Geschäftsmodelle, die die digitale Souveränität der Anwender·innen berücksichtigen, eröffnen völlig neue Erlösquellen. Wenn Nutzer·innen sich autonom dafür entscheiden, Daten unter den von ihnen gesetzten Bedingungen zu teilen, dann haben Unternehmen infolgedessen auch die Befugnis, diese Daten in gegenseitigem Einvernehmen zu verwerten. Hier bietet sich also für Unternehmen das Potenzial, sich neue datenbasierte Wertschöpfungsketten mit Alleinstellungsmerkmal zu erschließen, ohne dafür Schlupflöcher suchen zu müssen. Aus unserer Sicht sind datenbasierte Geschäftsmodelle sehr gut mit digitaler Souveränität vereinbar, auch wenn es bei den Anbieter·innen ein Umdenken erfordert.

Im Zuge unserer Nutzerstudie haben wir auch die Bereitschaft abgefragt, Geld zu zahlen, um bei einer für wichtig gehaltenen oder oft genutzten Anwendung die volle Kontrolle über die eigenen Daten zu haben. Fast 60 % würden dafür Geld in die Hand nehmen, bei den 18- bis 30-Jährigen ist der Wert mit über 9 € durchschnittlich am höchsten. Wie würden Sie dieses Ergebnis einschätzen? Liegt darin Potenzial für den breiteren Einsatz solcher Zahlmodelle?

Verschiedene Studien zeigen, dass sich die Nutzer·innen digitaler Plattformen grundsätzlich in unterschiedliche Gruppen hinsichtlich ihrer Präferenzen zum Thema Privatheit einteilen lassen: von unbekümmerten über kontrollbewusste bis hin zu stark privatheitsorientierten Nutzer·innen. Legten Nutzer·innen von sozialen Netzwerken in der Vergangenheit noch verstärkt Wert auf die Popularität und die Abwesenheit von Beitritts- und Mitgliedsgebühren digitaler Plattformen, so zeigt sich, dass aufgrund aktueller Entwicklungen und der sich häufenden Berichterstattung über Datenlecks zunehmend Zahlungsbereitschaften für Privatheit entstehen. Für Betreiber·innen digitaler Plattformen eröffnen sich dadurch Chancen für Wettbewerbsvorteile durch ein faires und transparentes Management von Privatheit in ihren jeweiligen Märkten.

Ihre Ergebnisse stimmen uns mit Blick auf die Zukunft sehr hoffnungsvoll, weil sie sehr eindrücklich zeigen, dass Datensouveränität für Bürger·innen einen Wert hat – und zwar insbesondere bei den Jüngeren. In Märkten, in denen viele vergleichbare Leistungen angeboten werden, kann Datensouveränität das entscheidende Differenzierungsmerkmal im Wettbewerb sein und Zahlungsbereitschaft bei potenziellen Kund·innen generieren.

Nur 41 % der Befragten sind der Meinung, dass es ausreichend datenschutzfreundliche Alternativen bei digitalen Anwendungen gibt.[III]

Im Projekt ViCon erforschen Sie Mensch-Technik-Dialoge für informierte Einwilligung in die Verarbeitung patientenbezogener Daten. Können Sie einen kurzen Einblick in das Projekt geben und auf die Frage eingehen, inwiefern Vertrauen bei der Datenweitergabe im Gesundheitsbereich eine Rolle spielt?

Daten spielen eine immer größer werdende Rolle für die Erbringung gesundheitsbezogener Dienstleistungen. Ihre Verarbeitung erfordert jedoch die Einwilligung der Patient·innen. Schon jetzt leisten diese z. B. bei einer stationären Aufnahme durchschnittlich zwischen acht und zehn Unterschriften ab. Offen ist, inwiefern Informiertheit und damit Souveränität bei den Patient·innen in Bezug auf Einwilligungen zur Verar-

[III] Basis: alle Befragten (n = 2000). Darstellung der Top 2. Frage Q20: Inwiefern stimmen Sie der folgenden Aussage zu? Es gibt ausreichend digitale Anwendungen, die datenschutzfreundlich sind.

beitung patientenbezogener Daten nicht nur angenommen werden kann, sondern auch erzielt wird.

Im Projekt ViCon soll ein virtueller Consent-Assistent entwickelt werden, der Bürger·innen dabei unterstützt, informierte Einwilligungen in die Verarbeitung ihrer patientenbezogenen Daten zu geben. Vertrauen spielt dabei eine sehr wichtige Rolle, insbesondere wenn die Entscheidung sich in den virtuellen Raum ohne das Beisein des Gesundheitspersonals verlagert. Ein Teilziel des Projekts ist es daher, Vertrauen im Kontext von eHealth zu messen und bei der Entwicklung des ViCon-Assistenten zu berücksichtigen. Dabei spielen Faktoren wie der Informationsgehalt, Merkmale der Organisation, gesellschaftlicher Einfluss, technologiebezogene Features sowie die Nutzerkontrolle eine sehr wichtige Rolle.

Dr. Marija Radić, Fraunhofer-Zentrum für Internationales Management und Wissensökonomie IMW
© Fraunhofer IMW

Dr. Marija Radić leitet die Abteilung „Unternehmensentwicklung im internationalen Wettbewerb“ und die Gruppe „Preis- und Dienstleistungsmanagement“ am Fraunhofer IMW. Im Rahmen dieser Tätigkeit forscht sie im Bereich der digitalen Dienstleistungs- und Geschäftsmodellentwicklung, der digitalen Gesundheitsversorgung und zur Nutzerakzeptanz beim Einsatz von Technik und datengetriebener Wertschöpfung.

In der Praxis: Mensch-Technik-Interaktion für Gesundheit und Selbstbestimmung *Interview mit Marie Kochsiek*

Sie haben mit drip eine datenschutzfreundliche Alternative für Zyklusapps entwickelt. Was war die Motivation dahinter und wie stellte sich der Entwicklungsprozess dar?

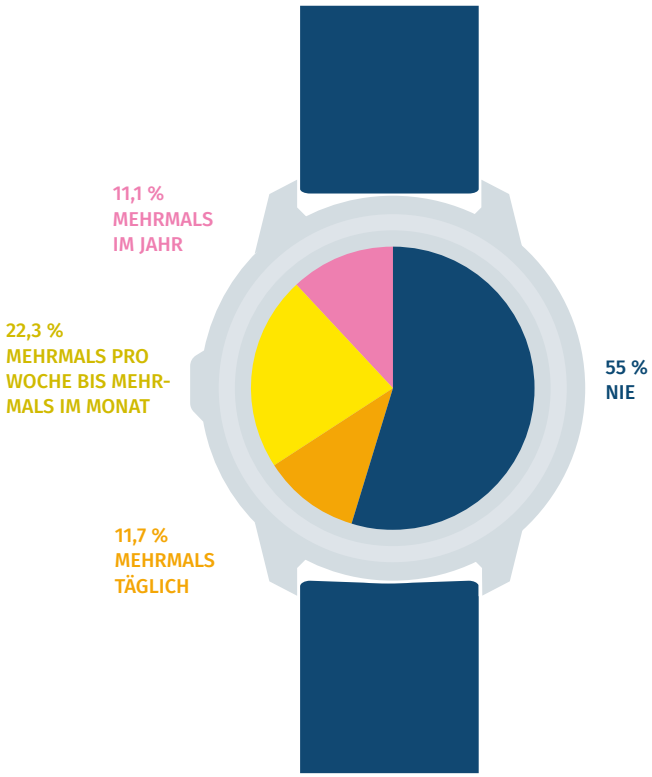
Marie Kochsiek: drip ist tatsächlich aus einer Nutzendenperspektive entstanden. Ich hatte mir selbst vor einigen Jahren eine Zyklusapp heruntergeladen – die erste, die mir im Smartphone-Store vorgeschlagen wurde. Eine Freundin hat mich dann aber am gleichen Tag auf die Datenschutzbestimmungen hingewiesen, woraufhin ich die App wieder gelöscht habe. Das Thema Datenschutz mit besonderem Fokus auf Zyklus und sexuelle Gesundheit hat mich aber seither nicht mehr losgelassen. In meinem Studium der Soziologie habe ich meine Abschlussarbeit zum Thema Zyklusapps geschrieben. Ich habe da eine Lücke erkannt – es gab noch nicht viel Literatur

und auch keine Anwendungen mit einem Fokus auf die technische Mündigkeit der Nutzenden. Diese Schieflage und mein Interesse an netzpolitischen Themen haben mich zu einem Kollektiv für Programmierer·innen in Berlin gebracht. Unterstützt vom Prototype Fund konnte ich 2018 gemeinsam mit Tina Baumann und Julia Friesel loslegen. Die sechs Monate der Förderung waren ein wichtiger Grundstein, um die drip-App Open Source und nichtkommerziell zu gestalten. Das war uns von Beginn an sehr wichtig.

Gab es technische Herausforderungen und standen die im Zusammenhang mit den Zielen der App, offen, datenschutzkonform und nutzerfreundlich zu sein?

Das ist eine spannende Frage, weil dahinter die Annahme steckt, dass es schwierig ist, diesen Weg zu wählen und Nutzungsdaten nicht zu verkaufen. Die Antwort darauf ist natürlich: „nein“. Dadurch, dass drip keine Daten sammelt, müssen wir auf technischer Ebene auch nichts damit tun. Wir brauchen keine Strukturen, um ethisch und konform mit Daten umzugehen, also sie zu speichern, zu verarbeiten oder sie weiterzugeben, da wir sie ja gar nicht erst haben. Worauf wir besonders Wert gelegt haben, war die Verwendung einer verschlüsselbaren Datenbank.

Nutzung von Fitnesstrackern und Gesundheits-Apps



Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q1. Wie oft nutzen Sie folgenden digitale Anwendungen? Fitnesstracker und/oder Gesundheits-Apps
© Ipsos | Digital Autonomy Hub

Wie sind Sie vorgegangen, um die App so zu gestalten, dass die Interessen der Nutzer·innen im Vordergrund stehen und die Interaktion mit der Technologie möglichst anwendungsfreundlich ist?

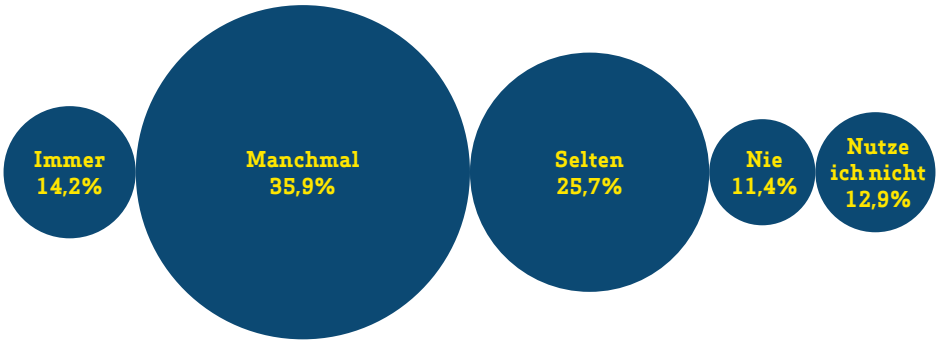
Das Besondere an unserem Team war ja, dass wir alle aus einer Nutzerinnenperspektive heraus die Anwendung gestaltet haben. Das mag banal klingen, aber ich kenne sonst keine Beispiele für Zyklusapps, bei denen das der Fall ist. Trotzdem war natürlich der Anspruch, nicht nur für uns selbst zu entwickeln, und wir haben gleich zu Beginn eine Umfrage gemacht, welche Kategorien und Symptome im Zyklustracking aufgenommen werden sollen.

Seitdem die App verfügbar ist, bekommen wir auch immer wieder Feedback von Nutzer·innen. Das versuchen wir natürlich zu berücksichtigen in der Fortentwicklung; wir sind inzwischen ein Kernteam von vier Personen, aber arbeiten alle ehrenamtlich daran. Der letzte große Meilenstein war ein Redesign, um die App anwendungsfreundlicher zu gestalten. Wir sehen auch, dass sich eine Community von Freiwilligen auf gitlab einfindet, die helfen, die App in unterschiedliche Sprachen zu übersetzen. Gerade bei einem so intimen Thema wie Zyklusgesundheit macht die Verfügbarkeit in der eigenen Sprache einen Unterschied für viele Menschen.

Wie werden Nutzer·innen und Ihre Community auf drip aufmerksam?

Wir machen keine klassische Werbung, aber versuchen nach Möglichkeit bei relevanten Veranstaltungen und in den Medien präsent zu sein und zu sensibili-

Nur wenige Befragte informieren sich konsequent vor dem Kauf oder der Installation einer Anwendung über deren Datenschutzfreundlichkeit.



Basis: alle Befragten (n = 2000). Angaben in Prozent. Frage Q12: Informieren Sie sich beim Kauf von digitalen Geräten (z. B. Fitnesstracker, Smart-home-Geräten, Smartphones), beim Installieren von Apps und bei der Nutzung von Social-Media-Plattformen darüber, wie datenschutzfreundlich diese sind? © Ipsos | Digital Autonomy Hub

sieren. Dabei geht es auch darum, die Zusammenhänge zwischen Technologie, Nutzer·innen, Gesellschaft, und Datenschutz darzustellen. drip ist ja nicht nur der Code, sondern vereint gewisse Werte und Ansätze, also zum Beispiel feministisch, kollektiv, nicht-kommerziell, datenschutzfreundlich und genderinklusiv zu sein.

Ein weiterer Aspekt in unserer Außenwirkung ist es, Menschen in ihrem digitalen Leben zu ermächtigen – nicht nur als Nutzer·innen, sondern auch als potenzielle Gestalter·innen von Technologie. Das finden viele ansprechend und sie teilen unsere Einschätzung, dass es großen Nachholbedarf in der informatischen Bildung und dem Technologieverständnis gibt. Wir wollen Berührungsängste mit Technik abbauen, indem wir sichtbar machen, dass Programmieren allen offen steht, anwendungsbezogen ist und Technologie nicht nur von einem bestimmten Typ Mensch gestaltet wird.

In unserer Umfrage gibt fast die Hälfte der Menschen an, Fitnesstracker oder Gesundheitsapps zu nutzen. Über ein Drittel der Nutzer·innen von digitalen Anwendungen informiert sich nie oder selten über die Datenschutzfreundlichkeit von Anwendungen. Die meisten geben an, Anwendungen oder Geräte zu nutzen, obwohl sie wissen, dass sie nicht datenschutzfreundlich sind. Können wir durch Technologie die digitale Souveränität steigern?

Spannend ist: Das Phänomen des „quantified self“ in Bezug auf Fitnesstracker wurde schon intensiv besprochen, aber Zyklustracking kam da gar nicht vor. Das Feature spielt in den meisten Gesundheitsapps keine Rolle, obwohl es einen signifikanten Teil der Bevölkerung interessiert oder beschäftigt. Das erklärt die inzwischen große Beliebtheit von Zyklusapps für Smartphones.

Hinter vielen dieser Apps stehen dann aber daten- bzw. werbebasierte Geschäftsmodelle, bei denen sogar eine gewisse Motivation besteht, dass Nutzer·innen die Technologie und dahinterstehende Unternehmen gar nicht allzu sehr hinterfragen. Gleichzeitig ist das Thema Zyklus nach wie vor tabuisiert und viele Menschen sind eher bereit, einer als neutral wahrgenommenen Technologie diese intimen Körperdaten mitzuteilen, als zum Beispiel mit dem Umfeld oder mit der eigenen Ärztin darüber zu sprechen. Deshalb ist es umso wichtiger, dass eine Anwendung eine unterstützende und aufklärende Funktion einnimmt und die Nutzer·innen so mündig macht. Unser Ansatz und Wunsch ist es, transdisziplinär zu arbeiten und auch Mediziner·innen in die Entwicklung und Nutzung miteinzubeziehen. Grundsätzlich muss man aber natürlich anerkennen, dass das eine komplexe Herausforderung ist, die nicht an einem Tag und nicht mit einer einzelnen Anwendung gelöst werden kann.

Marie Kochsiek,
Heart of Code e. V. und drip
© Marie Dietze

Marie Kochsiek ist als Software-Entwicklerin und Soziologin besonders interessiert an den Schnittstellen zwischen Gesellschaft, Technologie und sexueller Gesundheit. Sie ist Teil des feministischen Hackspace Heart of Code e. V. und baut mit drei weiteren Entwicklerinnen an drip, einer freien und quelloffenen App für Menstruation und Fruchtbarkeitstracking.

Danksagung

Das Team des Digital Autonomy Hubs bedankt sich herzlich bei allen Autor·innen und Interviewpartner·innen, die zu dieser Publikation beigetragen haben. Mit ihrer Expertise haben sie Aufschluss über vielfältige Aspekte des Themenkomplexes rund um individuelle digitale Souveränität gegeben und die dargestellten Umfrageergebnisse wesentlich bereichert. Wir bedanken uns bei unseren Berater·innen bei Ipsos, mit deren Hilfe wir die Umfrageergebnisse erzielen konnten, auf denen diese Publikation aufbaut. Wir bedanken uns bei allen, die zu Redaktion, Lektorat, Gestaltung und Layout der Publikation beigetragen haben. Unser herzlicher Dank gilt ebenfalls dem Bundesministerium für Bildung und Forschung, das dieses Projekt im Rahmen der Bekanntmachung „Mensch-Technik-Interaktion für digitale Souveränität“ fördert.

Das Digital Autonomy Hub – Technik souverän nutzen ist ein Kompetenzzentrum, das ein interdisziplinäres Netzwerk von 43 Instituten und Organisationen koordiniert. Der Hub macht sichtbar, woran die Partner forschen und welche Ideen sie entwickeln, um die individuelle digitale Souveränität zu stärken. Ziel dieses Wissenstransfers ist es, allen Menschen einen reflektierten und selbstbestimmten Umgang mit ihren Daten, Geräten und Anwendungen zu ermöglichen. Das Kompetenzzentrum bereitet aktuelle Forschungsergebnisse für Zivilgesellschaft, Politik, Wissenschaft und Wirtschaft auf und berät die verschiedenen Akteure zu ethischen, rechtlichen und sozialen Aspekten der Datennutzung. Das Digital Autonomy Hub wird vom Bundesministerium für Bildung und Forschung im Rahmen des Forschungsprogramms „Miteinander durch Innovation“ gefördert und von AlgorithmWatch und Gesellschaft für Informatik e.V. (GI) umgesetzt. Mehr Informationen unter: www.digitalautonomy.net