Souveräne digitalrechtliche Entscheidungsfindung hinsichtlich der Datenpreisgabe bei der Nutzung von Wearables

Arvid Butting[1], Niel Conradie[2], Jutta Croll[3], Manuel Fehler[4], Clemens Gruber[3], Dominik Herrmann[5], Alexander Mertens[6], Judith Michael[1](✉), Verena Nitsch[6], Saskia Nagel[2], Sebastian Pütz[6], Bernhard Rumpe[1], Elisabeth Schauermann[7] Johannes Schöning[8], Carolin Stellmacher[8] und Sabine Theis[6]

[1] Software Engineering, RWTH Aachen
{butting,michael,rumpe}@se-rwth.de
[2] Angewandte Ethik, RWTH Aachen
{saskia.nagel,niel.conradie}@humtec.rwth-aachen.de,
[3] Stiftung Digitale Chancen
{jcroll,cgruber}@digitale-chancen.de
[4] Garmin Würzburg GmbH, manuel.fehler@garmin.com
[5] Privatsphäre und Sicherheit in Informationssystemen, Universität Bamberg,
dominik.herrmann@uni-bamberg.de
[6] Institut für Arbeitswissenschaft, RWTH Aachen
{a.mertens,v.nitsch,s.puetz, s.theis}@iaw.rwth-aachen.de
[7] Gesellschaft für Informatik, elisabeth.schauermann@gi.de
[8] Human-Computer Interaction, Universität Bremen
{schoening,cstellma}@uni-bremen.de

Zusammenfassung. Wearables unterstützen ihre Nutzer:innen in unterschiedlichen Kontexten. Dabei erzeugen und nutzen sie eine Vielzahl von oft sehr persönlichen (Gesundheits-)Daten, ohne dass Nutzer:innen über die notwendigen Kenntnisse und Erfahrungen verfügen, um reflektierte Entscheidungen über die Nutzung dieser Daten treffen zu können. In der aktuellen Forschung fehlen Konzepte, die einen unreflektierten Datenaustausch vermeiden und reflektierte Entscheidungen unterstützen. In diesem Beitrag diskutieren wir gesellschaftliche Herausforderungen der digitalen Souveränität und zeigen mögliche Wege der Visualisierung persönlicher (Gesundheits-)Daten und der Interaktion mit einem System, das transparente Informationen über die Nutzung von Wearable-Daten liefert. Wir zeigen Möglichkeiten zur Visualisierung rechtlicher und datenschutzrechtlicher Informationen auf und diskutieren unsere Ideen für einen erlebbaren Datenschutz mit Gamifizierungskonzepten. Die Bereitstellung interaktiver und visueller Datenräume kann die Fähigkeit zur eigenständigen Selbstbestimmung für Datenpreisgaben stärken.

Schlüsselwörter: Digitale Souveränität · Datenschutz · Wearables · Fitnesstracker · Gesundheitsdaten · Visualisierung · InviDas.

1 Motivation

Wearables sind allgegenwärtig [6]. Mit Wearables bezeichnet man eine Gruppe von mobilen Geräten, die Nutzer:innen direkt am Körper tragen und mit einer Vielzahl von Sensoren ausgestattet sind, um sie mobil zu unterstützen [32,43]. Wearables können eine Vielzahl von Aktivitäten ihrer Nutzer:innen und deren Gesundheitsdaten aufzeichnen. Anwendungen existieren in einem breiten Spektrum von Bereichen, z. B. Gesundheit, Lebensstil, Arbeit, Fitness [36,28,4,39,40]. Diese Arbeit betrachtet Gesundheitsdaten aus Fitnesstrackern.

Gesundheitsdaten unterliegen nach der europäischen Datenschutzgrundverordnung (DSGVO [11]) einem besonderen Schutz und werden als besonders „sensibel“ wahrgenommen. Entsprechend hoch ist der Bedarf an einer verlässlichen und transparenten Grundlage für die einfache, reflektierte Entscheidungsfindung bei der Erhebung, Verarbeitung und Weitergabe von mit Wearables erhobenen Gesundheitsdaten [15,42]. Während z. B. Endanwender:innen durch die Verwendung eines Fitnesstrackers verstehen möchten, wie viel sie sich bewegen, wie viele Kalorien sie verbrennen und wie sich dies auf ihre Gesundheit auswirkt, könnten Hersteller und Drittanbieter aus diesen sensiblen Daten Rückschlüsse auf den Gesundheitszustand der Nutzer:innen ziehen, z. B. indem sie gemessene Bewegungsdaten mit weiteren persönlichen Krankheits- und Gesundheitsdaten kombinieren. Wenn Nutzer:innen z. B. die Begleitapplikation des Fitnesstrackers auf dem Smartphone installieren, können im Hintergrund zusätzliche Daten zwischen dem Smartphone, anderen Smartphone-Anwendungen und den Herstellern des Fitnesstrackers ausgetauscht werden. Oftmals sind diese Prozesse und deren Konsequenzen für Nutzer:innen nicht ausreichend transparent.

Dieser Beitrag diskutiert Probleme, auf die Menschen bei den aktuellen Formulierungen in Datenschutzerklärungen treffen und stellt erste Konzepte zum besseren Verständnis von ihrer Datenpreisgabe vor. Darüber hinaus zeigen wir erste Ideen für die Visualisierung der (Gesundheits-)Datennutzung von Fitnesstrackern, die im Rahmen des Projekts InviDas[9] entwickelt und umgesetzt werden. Im Projekt InviDas wird von einem interdisziplinären Expert:innenteam aus Informatik (Software Engineering, Sicherheit und Datenschutz, Human-Computer-Interaction), Kommunikationsdesign, Psychologie, Human Factors und Ergonomie, Ethik und Recht eine digitale Plattform entwickelt. Ziel der Plattform ist es, personenbezogene Daten, die ethischen und rechtlichen Implikationen ihrer Übermittlung und deren Verarbeitung für Nutzer:innen besser verständlich zu machen.

Im folgenden Abschnitt betrachten wir das Konzept digitale Souveränität und Herausforderungen für die Gesellschaft. Abschnitt 3 beschreibt aktuelle Herausforderungen beim Verständnis von Datenschutzerklärungen und zeigt alternative Konzepte auf. Abschnitt 4 diskutiert mögliche Visualisierungen zur Unterstützung der digitalen Souveränität. Abschnitt 5 behandelt verwandte Arbeiten. Der letzte Abschnitt bietet einen Ausblick in zukünftige Entwicklungen.

[9] Beschreibung des vom BMBF geförderten Projekts InviDas unter `https://technik-zum-menschen-bringen.de/projekte/invidas`

2 Digitale Souveränität – eine gesellschaftliche Herausforderung

Es ist wichtig, das Verständnis und das Vertrauen in die Datenerfassung von Wearables zu verbessern, um die Nutzer:innen in die Lage zu versetzen, auf einfache und effiziente, aber verständliche Weise informierte Entscheidungen zu treffen, um ihre digitale Souveränität aufzubauen und zu erhalten. Beginnen wir zunächst mit einer Diskussion dieses Konzepts.

2.1 Das Konzept digitale Souveränität

Reflektierte Entscheidungen, die von den Entscheidungsträger:innen auch im Nachhinein getragen werden können, erfordern nachvollziehbare Information als Entscheidungsgrundlage. Entscheidungsträger:innen, die Zusammenhänge und Funktionsmechanismen eines Systems nicht ausreichend nachvollziehen können, haben häufig keine Möglichkeit, diese Entscheidung durchdacht und selbstbestimmt zu treffen. Um eine rationale Entscheidung zu treffen, ist es wichtig, nachzuvollziehen, wie ein Sachverhalt zustande kommt [38]. Erst wenn digitale Vorgänge und Entscheidungen wahrnehmbar und nachvollziehbar sind, können Nutzer:innen verstehen, wem ihre Daten übermittelt werden, wozu welche ihrer Daten mittelbar und unmittelbar genutzt werden, und dann auch bewerten, ob sie diesen Nutzungen zustimmen möchten oder nicht.

Floridis Konzept der *digitalen Souveränität* ist das legitimer Kontrolle über das Digitale [14]. Diese Kontrolle wird als eine Art „Steuerungskontrolle“ verstanden, wie sie vom Kapitän eines Schiffes ausgeübt wird. Das Digitale geht über Daten hinaus und umfasst Elemente wie Prozesse und Standards. Diese Konzeption ist normativ zu verstehen, da es hier um eine legitime Kontrolle geht – nicht um die tatsächliche Kontrolle über das Digitale.

Wie in Kranich et al. [21] erklärt, stellt der Begriff der digitalen Souveränität häufig einen zivilrechtlichen und volkswirtschaftlichen Bezug her, obwohl die Handlungshoheit in digitalen Lebenswelten [41] mehr als das umfasst. Verfassungsrechtliche Interpretationen ergeben sich aus dem Begriff Souveränität: Er bezeichnet „oberste Gewalt“ oder „Souveränität des Staates“, aber auch die „Unabhängigkeit eines Staates vom Einfluss anderer Staaten“. Diese wird durch individuelle Faktoren bestimmt, die mit den rechtlichen, wirtschaftlichen und sozialen Bedingungen zusammenhängen. Mertz et al. [23] haben das Konzept der digitalen Souveränität mit den begrifflichen Komponenten Kompetenz, Informiertheit, Werte, Wahlmöglichkeit, Freiwilligkeit, Entscheidungs- und Handlungsfähigkeit beschrieben. Darüber hinaus werden technische, soziokulturelle und persönliche Determinanten identifiziert, d. h. Bedingungen und Faktoren, die empirisch untersuchen, inwieweit eine Person digital selbstbestimmt ist.

Auf individueller Ebene erfordern reflektierte Entscheidungen ausreichende Informationen als Grundlage für die Entscheidungsfindung. Entscheidungsträger:innen, die die Zusammenhänge und Funktionsmechanismen eines Systems nicht wahrnehmen und verstehen, haben keine Möglichkeit, diese Entscheidung

vernünftig und selbstbestimmt zu treffen. Nur wer verstehen und reflektieren kann, wie eine Situation tatsächlich abläuft, kann rationale, begründete Entscheidungen treffen. Nur wenn digitale Prozesse und Entscheidungen wahrnehmbar und nachvollziehbar sind, wenn Anwendungen nicht nur transparent sind, sondern auch den Nutzer:innen erklärt werden, können die Nutzer:innen verstehen, welche Daten gesammelt werden und wofür ihre Daten verwendet werden. Es ist ein wesentliches Merkmal zur Förderung der digitalen Souveränität, die Nutzer:innen in die Lage zu versetzen, die Informationen über ihre Daten zu verstehen und zu verarbeiten, und zwar in einer Weise, die für sie angemessen und aussagekräftig ist. In einer digitalisierten Gesellschaft ist die *digitale Souveränität* ein *wichtiger Aspekt* der *allgemeinen Souveränität*, zu der auch die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung der digitalen Systeme selbst, die in ihnen erzeugten und gespeicherten Daten und die Prozesse, die sie repräsentieren, gehört [34].

2.2 Digitale Souveränität und Wearables

Dies trifft in besonderem Maße auf Informationssysteme zu, die am Körper getragen werden. Solche so genannten Wearables zeigen nicht nur Benachrichtigungen vom Smartphone an und messen den Puls, sondern sie analysieren das Schlafverhalten, zählen Schritte, zeichnen Ort und Dauer von Trainingseinheiten auf und berechnen den Kalorienverbrauch. Ein Vermessen des persönlichen Verhaltens in seinen vielen Facetten wird möglich ("Quantified Self"). Die Daten diverser Endgeräte können auf Plattformen zusammengeführt werden, um ein komplexes Profil der Nutzenden und deren Umgebung zu erstellen. Anders als bei Nachrichten und Bildern, die in sozialen Medien geteilt werden, handelt es sich bei den durch Wearables erhobenen Daten oftmals um sensible biometrische Gesundheitsdaten. Entsprechend hoch ist der Bedarf der Nutzer:innen nach einer Grundlage für die erleichterte, reflektierte Entscheidungsfindung zur Sammlung, Verarbeitung und Weitergabe ihrer Daten. Während die Endverbraucher:innen durch die Nutzung eines Fitness-Armbandes beispielsweise verstehen möchten, wie viel sie sich bewegen, wie viele Kalorien sie verbrennen und wodurch ihr Bewegungsverhalten beeinflusst wird, könnten Hersteller:innen und Drittanbieter:innen z.B. durch die Kombination der dabei gemessenen Bewegungsdaten mit personenbezogenen Krankheits-und Gesundheitsdaten Rückschlüsse auf den Gesundheitszustand der Nutzer:innen ziehen. Installieren die Endverbraucher:innen die zum Fitness-Armband passende App auf ihrem Smartphone, können die Daten unter Umständen im Hintergrund mit anderen Apps und deren Anbietern ausgetauscht werden (vgl. ein aktuelles Experiment der Washington Post[10] zur iOS-Hintergrundaktivität). Diese digitalen Prozesse, aber auch rechtliche Zusammenhänge, bleiben jedoch oft unsichtbar und damit unverstanden.

[10] `https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/`. Letzter Zugriff: 23.10.2020

Darüber hinaus haben auch bereits Versicherungen oder Arbeitgeber Interesse an diesen Daten geäußert[11]: Workplace-Wellness Programme sollen Mitarbeiter:innen sowie ihre Familienmitglieder dazu zu ermutigen, einen gesunden Lebensstil zu führen. Andere Überlegungen betreffen die Kopplung der Krankenversicherungsbeiträge an die Fitness der Versicherten. Wer seinen Gesundheitszustand verbessert wird mit Boni belohnt.

Ein Ziel der europäischen Datenschutzgrundverordnung (DSGVO) ist es, die Interessen der Nutzenden gegenüber datengetriebenen Plattformen und Technologien zu stärken. Diese wichtige rechtliche Schnittstelle zwischen Menschen und Technologie wird derzeit meist über lange, komplizierte und textuelle Datenschutzerklärungen und -einwilligungen abgebildet. Die Texte enthalten oft fachspezifische Formulierungen, die juristischen Anforderungen genügen müssen. Die für eine informierte Einwilligung notwendigen Informationen sind schwierig zu extrahieren. Das Lesen und kritische Hinterfragen ist aufwändig und selbst bei entsprechender Bereitschaft fehlt vielen die rechtliche und technische Expertise, um die Formulierungen ausreichend nachvollziehen und deren Bedeutung für die eigenen Daten interpretieren zu können. Oft wird daher dem Nutzungsinteresse Vorrang gegeben und den Bedingungen zugestimmt, ohne dass die Inhalte verstanden wurden: Entscheidungen über die Verarbeitung sensibler persönlicher Daten durch Wearables (z. B. Aufenthaltsort, Herzfrequenz, Schlaf-und Wachzyklen) werden so oft leichtfertig getroffen, da die vorliegende Information als zu lang und schwer rezipierbar wahrgenommen und deshalb ignoriert wird. Vulnerable Anwender:innen wie sehr junge Nutzer:innen oder Menschen mit kognitiven Beeinträchtigungen können häufig keine bewusste, reflektierte Einwilligung in die Nutzung ihrer Daten geben. Ältere Nutzer:innen hingegen lehnen die Nutzung ab, weil sie nicht nachvollziehen können, wie welche personenbezogenen Daten über sie erfasst werden und welche Konsequenzen dies für sie haben kann oder übertragen die Entscheidung dafür bei der Einrichtung der Systeme jüngeren, Technik-affineren Familienmitgliedern.

2.3 Ziele des Projekts InviDas

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt InviDas (Interaktive, visuelle Datenräume zur souveränen, datenschutzrechtlichen Entscheidungsfindung) möchte die individuelle Souveränität im digitalen Kontext durch interaktive Datenvisualisierungen persönlicher Gesundheitsdaten und datenschutzrechtlicher Informationen fördern. Derzeit liegen keine Erkenntnisse dazu vor, auf welcher Basis die Entscheidung zur Nutzung digitaler Endgeräte für ein aktiveres und gesünderes Leben getroffen wird, welche Kompetenzen und persönlichen Eigenschaften die Voraussetzung einer bewussten und zielführenden Entscheidung sind und wer die benötigten Kompetenzen wo und in welcher Form erwirbt. Um einer Spaltung in Menschen, die das Potenzial von gesundheitsfördernden digitalen Anwendungen nutzen, und weniger digital affine

[11] `https://futurezone.at/digital-life/versicherungen-ueberwachen-kunden-per-fitnesstracker/48.932.295`. Letzter Zugriff: 23.10.2020

Menschen, die davon nicht profitieren können entgegenzuwirken, bedarf es der partizipativen Entwicklung von Konzepten, die allen potenziell Interessierten im Hinblick auf die Nutzung von digitalen Gesundheitssystemen und Endgeräten eine kontextbewusste Entscheidung ermöglicht.

Im Spannungsfeld zwischen verweigerndem Technikpessimismus und unreflektierter Datenfreigabe gibt es Innovationsraum für eine nutzergerechte Gestaltung der Mensch-Technik Interaktion mithilfe von interaktiver Datenvisualisierungen, die Potenzial für eine gemeinwohlorientierten Technikentwicklung europäischer Prägung birgt. Es gibt bereits Ideen, Einverständniserklärungen und Datennutzungserklärungen mit statischen Icons zu bebildern[12], um diese besser verständlich zu machen. Das Projekt InviDas geht einen Schritt weiter und erforscht interaktive und visuelle Datenräume, um Einverständniserklärungen und Datennutzungserklärungen verständlich und erlebbar zu machen. Interaktive Visualisierungen sind in der Lage, komplexe Zusammenhänge durch grafische Darstellungen der gesammelten Daten abzubilden. Bisher nicht sichtbare Zusammenhänge werden dadurch nachvollziehbar. Im konkreten Anwendungsfall der Wearables soll unter Zuhilfenahme verschiedener nutzerzentrierter Datenvisualisierungen auf einen Blick dargestellt werden, wie umfangreich ein Datenprofil der Tragenden ist, welche Rückschlüsse beispielsweise auf Krankheiten gezogen werden können und welche Akteurinnen und Akteure auf welche Daten zugreifen können. Bisher existieren solche Nutzerprofil-Repräsentationen nur in nüchterner Textform, was die Verständlichkeit einschränkt und Interaktionsmöglichkeiten begrenzt. Rechtliche Informationen und Folgenabschätzung sind hierbei bisher noch nicht realisiert worden. Dazu werden innerhalb des Projektes rechtliche und ethische Parameter definiert und für die Nutzenden abgebildet, um ihnen eine bessere Entscheidungsgrundlage für souveränes digitales Handeln zu geben.

Das InviDas-Projekt entwickelt eine digitale Plattform, über die personenbezogene Daten sowie die datenschutzrechtlichen Implikationen ihrer Weitergabe und Verarbeitung verständlicher gestaltet werden. Menschen unterschiedlicher Technikgenerationen und Altersgruppen soll geholfen werden, abstrakte technische und rechtliche Zusammenhänge zu verstehen und folglich bewusste und reflektierte Entscheidungen zu treffen. Visuelles, interaktives Erleben der bisher unsichtbaren digitalen Prozesse soll das Technikverständnis, -vertrauen und die Souveränität digital-rechtlicher Entscheidungsfindungen verbessern. Dies wird durch einen visuellen spielerischen Zugang erreicht, der auf Nutzer:innenbedarfen basiert. Die Erkenntnisse und Instrumente aus InviDas sollen einer breiten Öffentlichkeit zur Verfügung stehen, den gesellschaftlichen Diskurs über digitale Souveränität bei Gesundheitsdaten voranbringen und mit Hinblick auf Übertragbarkeit und Generalisierbarkeit gesamtgesellschaftlich verwertet werden.

Zusammengefasst konzentriert sich das Projekt InviDas somit auf drei Ziele:

Z1) die Erforschung geeigneter Mechanismen zur Verbesserung der Übersicht über bzw. der Kontrolle über die Weitergabe der eigenen Daten bei der Nutzung von Wearables,

[12] `https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/`. Letzter Zugriff: 23.10.2020

Z2) das Entwickeln von Lösungen zum besseren Verständnis für und den Vergleich von Datenschutzerklärungen sowie
Z3) Lösungen zum Aufbau von digitaler Kompetenz zur Ermöglichung von reflektierten Nutzungsentscheidungen.

3 Analyse bestehender Datenschutzerklärungen

Um ein besseres Verständnis über die aktuelle Darstellung der Datenschutzerkärungen zu bekommen, haben wir für Deutschland geltende Datenschutzerklärungen namhafter Hersteller der meist verkauften Wearables (in alphabetischer Reihenfolge: Apple, FitBit, Fossil, Garmin, Huawei Samsung und Xiaomi) analysiert und hinsichtlich der enthaltenen Datenschutzkonzepte untersucht. Diese Analyse spiegelt jedoch nicht die Gesamtheit der Datenverarbeitung wider, weil Nutzer:innen während der Verwendung der Wearables der Verarbeitung weiterer Daten einwilligen können. Dies kann zum Beispiel geführt durch die Benutzerschnittstelle in der Menüführung oder durch die Anbindung an Drittanbieter-Software oder eine Companion App geschehen. Solche Entscheidungen sind nicht notwendigerweise Teil der Datenschutzerklärung.

Datenschutzerklärungen geben Auskunft über die *Datenart* der verarbeiteten Daten. Diese ist allerdings häufig nur exemplarisch angegeben und variiert in der Abstraktion. So werden Aussagen etwa teils im Bezug auf personenbezogene Daten getroffen und teils deutlich konkreter, zum Beispiel über das Geburtsdatum. Eine geeignete Darstellung und Kategorisierung der verschiedenen Datenarten stellt eine Herausforderung für das InviDas Projekt dar.

Die *Datenverarbeitungsform* bestimmt, was mit den erfassten Daten geschieht (siehe DSGVO Artikel 4(2)). Häufig erwähnte Formen der Datenverarbeitung in Datenschutzerklärungen beinhalten das Erheben, Verändern, Speichern, Weitergeben, und Löschen von Daten.

Die meisten Aussagen innerhalb von Datenschutzerklärungen werden über Daten getroffen, deren *"Dateneigentümer"* (wir verwenden der Verständlichkeit halber diesen Begriff wenngleich es ihn im juristischen Sinn nicht gibt) die jeweiligen Nutzer:innen sind. In einigen Ausnahmen werden aber auch Aussagen über Daten von dritten Personen, wie etwa durch freigegebene Kontakte getroffen.

Daten können aus verschiedenen *Datenquellen* erfasst werden. So kann etwa die manuelle Dateneingabe, die z.B. häufig für die Erfassung von Alter und Geschlecht verwendet wird, von der automatischen Erfassung von Daten über Sensoren (z.B. Position via GPS) unterschieden werden. Weiterhin gibt es Daten, die aus anderen (Roh-)Daten abgeleitet werden.

Der *Datenempfänger* ist meist das Unternehmen, welches Hersteller des Wearables ist oder wird als „Drittanbieter“ angegeben. In einigen Fällen, zum Beispiel bei der Realisierung von Coaching Services, können auch andere Nutzer:innen bzw. andere Rollen von Nutzer:innen Datenempfänger sein.

Der *Verarbeitungszweck* begründet, warum Daten verarbeitet werden. Das „berechtigte Interesse“ stellt hierbei die Rechtsgrundlage für die Datenverarbeitung Sinne der DSGVO dar. Ausprägungen hiervon sind etwa die Notwendigkeit

zur Erbringung einer Dienstleistung oder zur Realisierung einer Funktion. Daten können aber auch z.B. für Marktforschung, dem Erstellen von Nutzerprofilen, oder zur Einhaltung von gesetzlichen Vorschriften verarbeitet werden.

In manchen Fällen gibt es eine *Nutzungsentscheidung*, die Nutzer:innen über die Verarbeitung der Daten treffen können. Wenn es eine Entscheidung gibt, basiert diese meist entweder auf dem Opt-In oder Opt-Out Prinzip. Opt-In ist zum Beispiel eine Funktion oder ein Dienst, der von Nutzer:innen aktiviert werden kann und durch den dann Daten verarbeitet werden. Dementgegen steht das Opt-Out für das Widerrufen einer Einerständniserklärung der Datenverarbeitung durch Nutzer, zum Beispiel durch das Deaktivieren einer Funktion oder das Abmelden aus Emailverteilern.

Datenschutzerklärungen enthalten unterschiedliche Aussagen zu den *Datenschutzmaßnahmen*, die das Unternehmen trifft. Zum Beispiel versprechen einige Anbieter, dass physische und technische Schutzmaßnahmen getroffen wurden, dass Daten verschlüsselt übertragen werden, oder dass Daten auf Servern innerhalb der EU gespeichert werden.

Die *Datenaufbewahrungsdauer*, sofern sie angegeben ist, bestimmt die Länge des Zeitraums zwischen Datenerfassung und -löschung. Häufig wird erwähnt, dass Daten nur so lange aufbewahrt werden, wie es für die Erfüllung von gesetzlichen Vorgaben erforderlich ist. In manchen Fällen werden Daten allerdings auch aufbewahrt, bis Nutzer:innen ihren Account explizit löschen.

Als *Rechtsgrundlage* für die Verarbeitung von Daten werden Buchstaben aus Artikel 6(1) der DSGVO herangezogen.

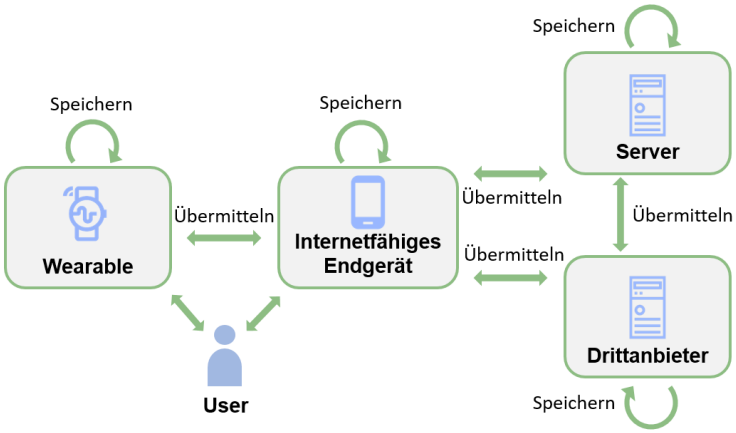

Abb. 1. Typische Konstellation von Datenverarbeitungsorten für Wearable-Anwendungen.

Insgesamt sind die Aussagen über die Datenverarbeitung in Datenschutzerklärungen häufig generell formuliert und beinhalten selten Zusammenhänge zwischen oben genannten Kategorien. So ist im Allgemeinen etwa nicht nachvoll-

ziehbar, für welche verschiedenen Zwecke jede Art von erhobenen Daten (z.B. Herzfrequenz) verwendet werden, an wen sie weitergegeben werden können, und wo sie verarbeitet werden. Zudem ist im Allgemeinen nicht nachvollziehbar, ob für eine konkrete Datenart z.B. die auf einem Fitness Armband ermittelte Herzfrequenz lokal auf dem Armband gespeichert, zu einem Mobiltelefon übertragen, oder auf einem Server hinterlegt wird. Somit ist aktuell in Datenschutzerklärungen nicht gut nachvollziehbar, welche Daten an welche beteiligten Orten, wie in Abbildung 1 dargestellt, verarbeitet werden. Dies sind jedoch Informationen, die sich Nutzer:innen erwarten würden.

4 Be- und ergreifbarer Datenschutz

Aktuelle und zukünftige Nutzer:innen von Wearables können durch die in InviDas entwickelte Plattform mit unterschiedlichen Hilfestellungen bei der Entscheidungsfindung unterstützt werden: Übersichtliche Darstellungen von gesammelten Fitnessdaten ermöglichen den Vergleich unterschiedlicher Anbieter, textuelle Datenschutzrichtlinien werden zu einem interaktiven, visuellen Raum umgewandelt um sie verständlich zu machen und Auswirkungen von Datenschutzpräferenzen werden in einem virtuellen „Escape Room“-Spiel erlebbar.

Zunächst erhalten die Nutzer in der Komponente *myDataCockpit* (Ziel Z1) einen Überblick über die von Wearables gesammelten Daten. In diesem Zusammenhang verwenden wir einen modell-basierten Software-Engineering-Ansatz mit Code-Generierung [16], um die Plattform zu schaffen. Die Plattform wird sowohl personenbezogene Daten, Kontextinformationen [25] als auch datenschutzrechtliche Metadaten verarbeiten und sich insbesondere auf die Frage konzentrieren, welche Daten mit wem und zu welchem Zweck ausgetauscht werden [24]. So soll den Nutzer:innen auch ermöglicht werden rückwirkend den Weg nachzuvollziehen, den ihre Daten im Verlauf der Verarbeitung durch andere Parteien genommen haben. Zu diesem Zweck wird ein geeignetes Metamodell erstellt und für die Generierung der Plattform verwendet, das aus einem Backend mit Datenspeicherung, einem Anwendungskern, einer Sicherheitsinfrastruktur und einem modernen visuellen Frontend besteht. Aufgrund des modell-basierten Entwicklungsansatzes können iterativ neue Daten und Metadaten eingebunden werden.

myDataCockpit kann entweder mit persönlichen Daten, die über ein Wearable gesammelt wurden, oder mit vordefinierten Daten von beispielhaften Nutzer:innen verwendet werden. Diese beispielhaften Nutzer sollten verschiedene Nutzer:innengruppen repräsentieren, z.B. ältere Menschen, die das Wearable zur Verfolgung ihrer täglichen Schritte verwenden, oder Marathonläufer, die sich auf einen Wettkampf vorbereiten. Welche Nutzer:innengruppen von Relevanz sind, bedarf weiterer Untersuchungen. Eine erste Grundlage bieten hierbei die Nutzer:innengruppen des D21-Index [1].

Abbildung 2 zeigt eine mögliche Visualisierung von Datenverarbeitungsorten. Wählt man einen bestimmten Datensatz aus, wie z. B. die Herzfrequenz, so erhält man Informationen über (1) die Sensorik zur Erfassung, (2) die Speicherung und Verarbeitung in den unterschiedlichen Komponenten (Fitnesstracker, zugehöri-

ge lokale Fitness-App am Smartphone, Server des Anbieters, Drittanwendungen) oder (3) die simulierten Datenübermittlungen zwischen den Komponenten. Zur leichteren Vergleichbarkeit von unterschiedlichen Anbietern könnten deren Datenverarbeitungsorte auch gegenübergestellt werden.

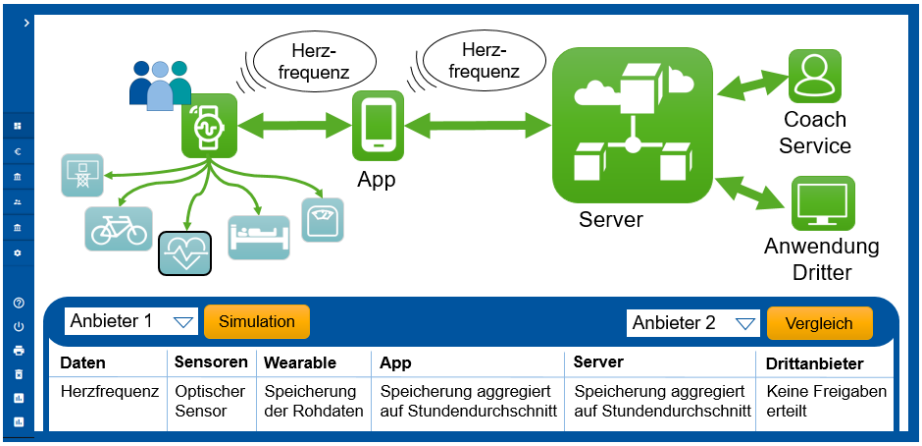

Abb. 2. Beispielhafte Anzeige: Graphische und tabellarische Darstellung von Verarbeitungsorten, Sensoren und Vergleich von Anbietern.

myDataSim ermöglicht es den Nutzern, die Konsequenzen für die Akzeptanz von Datenschutzrichtlinien verschiedener Anbieter (Ziel Z2 und Z3) anhand von Visualisierungen verschiedener Datenschutzrichtlinien sowie von Gamifizierungskonzepten zu verstehen. Textuelle Datenschutzrichtlinien werden zu einem interaktiven, visuellen Raum, in dem das eigene Datenprofil in ein sich veränderndes physisches Objekt transformiert wird. Diese Räume werden speziell an die verschiedenen Nutzer:innengruppen angepasst, z.B. jüngere oder ältere, erfahrene oder unerfahrene, skeptische, gelegentliche oder leidenschaftliche Nutzer:innen.

Ein virtuelles „Escape-Room“-Spiel ermöglicht es den Nutzer:innen die Auswirkungen von Entscheidungen zu erfahren, die sich auf die Verwendung ihrer Daten beziehen (Ziel Z3). Jede Entscheidung in einer Datenschutzrichtlinie ist mit einem Rätsel oder einem Satz ähnlicher Rätsel verbunden z.B. die Auswahl „Weitergabe der GPS Daten“ mit einem Rätsel verbunden, das auf Basis solcher GPS Informationen raten lässt, wo eine Beispielperson wohnt bzw. wo sich die Person oft aufhält. Im „Escape-Room“ müssen mehrere Rätsel gelöst werden, um den Raum verlassen zu können - was von den Entscheidungen der Nutzer:innen in Bezug zu deren Daten abhängt. Alle getroffenen Entscheidungen werden auf einer Skala bewertet. Diese Skala ist mit einer anderen „Welt“ verbunden, in der die Nutzer:innen den „Escape-Room“ verlassen können. Unterschiedliche Entscheidungen über die gemeinsame Nutzung tragbarer Daten wirken sich also auf die Welt aus, in die die Nutzer:innen den „Escape-Room“ verlassen. Abbildung 3

zeigt diese Grundidee für das virtuelle „Escape-Room“-Spiel. Durch diese Form der Gamifizierung [19] können die Nutzer:innen trainieren, wie sie die Auswirkungen auf ihre Daten beeinflussen, z. B. wie sie sie vor Manipulation schützen können, und so auf spielerische Weise ihre digitale Souveränität entwickeln und verbessern können.

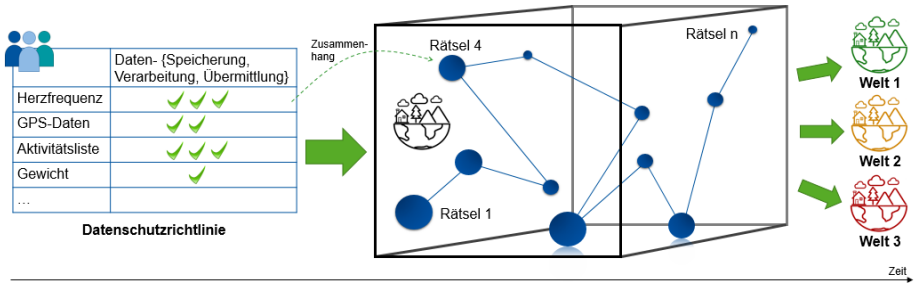

Abb. 3. Konzept des Escape-Room Spiels.

myDataCockpit und myDataSim können unabhängig voneinander eingesetzt werden und ermöglichen (a) den Vergleich verschiedener Produkte hinsichtlich ihrer Datenschutzrichtlinien für InteressentInnen und (b) das bessere Verständnis für Datenschutzerklärungen an Hand eigener Daten. Wir gehen davon aus, dass eine adäquate Vergleichsmöglichkeit eine wichtige Voraussetzung darstellt, um langfristig einen Wettbewerb um datenschutzfreundlichere Produkte zwischen den Herstellern von Wearables voran zu treiben.

5 Verwandte Arbeiten zur Visualisierung der individuellen digitalen Souveränität

Im Prinzip können sich die Nutzer:innen digitaler Dienste und Technologien derzeit über Datenschutzerklärungen informieren, um zu verstehen, was mit den Daten geschehen ist. In der Praxis kommt das jedoch nicht sehr oft vor. In der Regel akzeptieren die Nutzer:innen ihre Vereinbarungen, ohne sie durchzulesen [12,29]. Eine geeignete Visualisierung und strukturierte Präsentation kann ein Schlüsselfaktor zur Verbesserung dieser [3,30] sein. Daher erörtern wir in diesem Abschnitt verwandte Arbeiten zur Visualisierung von Rechtsinformationen sowie zur Visualisierung von Datenschutzmaßnahmen im Allgemeinen. Daran schließt sich eine Skizze von Ideen an, die im Rahmen des InviDas-Projekts entwickelt wurden, wie neuartige und greifbare Wege zur Visualisierung der Nutzung von (Gesundheits-)Daten, insbesondere von Wearables, geschaffen werden können.

5.1 Visualisierung von Rechtlichen Informationen

Im Bereich des Rechts und der Rechtsprechung [3] sind textliche Informationsdarstellungen vorherrschend. Rechtsvisualisierungen und bildliche Darstellungen von Rechtsinformationen sollen, da sie oft mühsam zu verstehen sind, die Kommunikation zwischen Fachleuten und Laien verbessern, um Kommunikationsfehler zu vermeiden [30]. Obwohl es kein allgemeines Modell für die Visualisierung von Rechtsdaten gibt, machen bildliche Darstellungen von Rechtsinformationen bestimmte rechtliche Aspekte besser verständlich. Mögliche Rechtsbegriffe, die mit Hilfe von Visualisierungen veranschaulicht werden können, sind z.B. Gerichtsverfahren, Rechtsquellen und Rechtsnormen oder juristische Personen wie Kaufverträge [37,22,9]. Typische Visualisierungstypen, die in diesem Zusammenhang verwendet werden, sind Flussdiagramme, Prozessmodelle, Comics und Metamodelle [17,31]. Wichtige Kriterien, die berücksichtigt werden müssen, sind u. a. die logische Abfolge von Rechtsprozessen, die Einhaltung der Rechtsordnung, die Angemessenheit, die Erkennbarkeit sowie die Verbindung zwischen Text und Bild [37]. Insbesondere letzteres ist von zentraler Bedeutung, da juristische Visualisierungen in der Regel in hybrider Form auftreten, d. h. Text und Bild erscheinen kombiniert, um die Wirksamkeit der Kommunikation zu erhöhen [3]. Ein iterativer Gestaltungsprozess für eine Visualisierung in einem rechtlichen Kontext umfasst vier Aspekte: (1) die Identifizierung von Nutzerbedürfnissen durch Beobachtung und Einfühlungsvermögen; (2) eine Definition der Projektziele durch Kommunikation, Visualisierung und Prototyperstellung; (3) eine effektive Sprache durch vereinfachte Kommunikation; (4) Anpassung an Zielgruppen mit multiplen Bedürfnissen durch visuellen Diskurs und Unterstützung rechtlicher Funktionen durch einen optimalen Mix aus Sprache und Grafik [3,31]. Lettieri et al. entwickelten die Webanwendung „Knowlex“ zur Visualisierung von Recherchen und zur Analyse juristischer Dokumente aus verschiedenen Quellen [22]. Die Ergebnisse der Studie (n=13) zeigten, dass die auf einem grafischen Ansatz basierende Unterstützung die Nutzer:innen in die Lage versetzt, ihre Aufgaben schneller und effektiver zu erledigen. Darüber hinaus waren die persönliche Einstellung und der persönliche Nutzen wichtige Faktoren, um die Akzeptanz der Software zu erhöhen. Darüber hinaus stellten Burkhardt und Nazemi in einer Studie, die auf einer juristischen Konzeptontologie [7] basierte, einen Norm-Grafik-Visualisierungsansatz vor. Durch die enge Zusammenarbeit mit Nutzer:innen sowie Rechtsexperten erhielt die Einführung des Rahmenkonzepts konstruktives Feedback und sogar positive Rückmeldungen in Bezug auf Produktivität und Nutzen. Die empirische Evaluation dieses Ansatzes bleibt jedoch eine große Herausforderung.

5.2 Visualisierung von Persönlichen Informationen

Die Visualisierung von Sicherheitsdaten spielt in vielen Bereichen der Informationssicherheit eine Rolle, wie z.B. Sicherheitsmetriken, Sicherheitsüberwachung, Erkennung von Anomalien, Forensik und Malware-Analyse. Informationswissenschaft, maschinelles Lernen und explorative Datenanalyse untersuchen

auch die Visualisierung von Sicherheitsdaten [2]. Ein Teilbereich der Visualisierung von Sicherheitsdaten ist die Visualisierung von Daten im Kontext der Cybersicherheit [27], die aufgrund der steigenden Zahl von Angriffen besondere Aufmerksamkeit erfährt [27,33]. Hier werden Daten für die Logdaten-Analyse, Port-Scans und Schwachstellenbewertung durch Visualisierungstypen wie Koordinatensysteme und Baumstrukturen [8] verständlicher. Fan et al. [13] schlagen ein Echtzeit-Netzwerksicherheitssystem vor, das unbeaufsichtigtes Lernen und Visualisierungstechnologie kombiniert, Netzwerk-Verhaltensmuster identifiziert und ein Visualisierungsmodul zur interaktiven Modellanpassung bereitstellt. Analyst:innen können mehrere Ansichten verwenden, um Erkennungsergebnisse schnell zu bewerten und Modelle anzupassen, um die Genauigkeit zu erhöhen [13].

Darüber hinaus gibt es Ansätze für die Visualisierung von datenschutzbezogenen Daten für Nutzer:innen, die oft als Transparenzverbessernde Tools (engl. Transparency Enhancing Tools, TETs) bezeichnet werden [26]. So entwickelten Kolter et al. z. B. eine Web-Browser-Erweiterung für die Visualisierung früherer Offenlegungen persönlicher Nutzerdaten, dargestellt in graphenbasierten Ansichten [20]. Bier et al. haben ein Privacy Dashboard entwickelt, das persönliche Daten entlang von Informationsflüssen visualisiert [5]. Van Kleek et al. visualisieren das Profil einer Person auf der Grundlage der Dauer ihrer App-Nutzung als navigierbare, gestapelte Balkendiagramme und von welchen Host-Server-Standorten diese Apps betrieben werden auf einer Weltkarte [35]. Kelley et al. [18] entwickelten ein Label ähnlich der Nährwertkennzeichnung auf Lebensmitteln um Datenschutzaspekte zu vermitteln. Emami-Naeini et al. [10] verfolgen einen ähnlichen Ansatz für ein IoT-Security-und-Privacy-Label.

6 Zusammenfassung und Ausblick

Die vielfältigen Herausforderungen und Spannungsfelder, die in diesem Projekt bearbeitet werden, erfordern einen inter- oder transdisziplinären Ansatz, um die sozio-technischen Systeme und Zusammenhänge in all ihren sozialen, rechtlichen und technischen Aspekten adäquat modellieren und interpretieren zu können. Mit einem entsprechend vielfältigen Methodenrepertoire, wie es vom Konsortium vertreten und in dieser Publikation diskutiert wird, ist es möglich, die vielfältigen Wechselwirkungen und Zusammenhänge bei der Entwicklung einer digitalen Plattform zu berücksichtigen, die visuelle, interaktive Erfahrungen ermöglicht, um den Nutzer:innen das Verständnis des Datenschutzes zu erleichtern.

Die Ziele, die hier verfolgt werden, wie Nutzerzentriertheit, technische Innovation, wirtschaftliche Konnektivität, digitale Politikreflexion, kontinuierliche ethische, soziale und rechtliche Analyse, sind so vielfältig wie die dafür erforderlichen Disziplinen. So müssen nicht nur die sozialen und rechtlichen Herausforderungen angegangen werden, sondern auch die Art und Weise, wie die Visualisierung rechtlicher Informationen oder von Informationen zum Schutz der Privatsphäre technisch umgesetzt wird, bedarf weiterer Forschung, denn nur eine effiziente methodologische und werkzeuggestützte Unterstützung wird es vie-

len Entwicklern soziotechnischer Systeme ermöglichen, ähnliche Visualisierungen einzubauen. Die Verwendung geeigneter Modelle der Visualisierungstechnik sowie der visualisierten rechtlichen oder datenschutzrechtlichen Datenstrukturen und ihrer konkreten Daten wird ein Schlüssel zur Bewältigung solcher Entwicklungsherausforderungen sein.

Vielen bisher praktizierten sozio-technischen Lösungen mangelt es an Zugänglichkeit für die komplexen Entscheidungsprozesse und die Abschätzung der Auswirkungen auf die einzelne Person und schließt damit viele Menschen davon aus, reflektierte Entscheidungen über die Nutzung und Verarbeitung ihrer persönlichen Daten treffen zu können. Die in diesem Beitrag vorgestellten ersten Ideen und Konzepte leisten einen methodischen und operationellen Beitrag zur Verringerung dieser digitalen Kluft im Kontext Wearables. Aufgrund der zunehmenden Verbreitung von tragbaren Sport- und Gesundheitstechnologien, aber auch in der Fertigung und Produktion, ist davon auszugehen, dass die Nachfrage in Zukunft steigen und immer mehr Menschen betreffen wird. Aufgrund des integrierten Ansatzes werden die Ergebnisse eine Verallgemeinerung auf andere Anwendungsbereiche ermöglichen, so dass in Zukunft auch die Nutzer:innen anderer Technologien und Dienstleistungen von mehr Transparenz und digitaler Souveränität profitieren werden. Darüber hinaus werden die technologisch-technischen Projektergebnisse in allen vertretenen Disziplinen in die wissenschaftliche Forschung einfließen und stellen dank des hohen Innovationsgrades einen wichtigen Beitrag zum Diskurs dar. Letztlich soll damit ein Weg zwischen Technologiepessimismus und reflexionsfreiem Datenaustausch eröffnet werden, der den Raum für Innovationen für benutzerfreundliches Design weiter öffnet.

Referenzen

1. Wie Digital Ist Deutschland? Initiative D21 e.V (2019), https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/wie-digital-ist-deutschland
2. Balakrishnan, B., et al.: Security data visualization. SANS Institute In-foSec Reading Room (2015), https://www.sans.org/reading-room/whitepapers/metrics/security-data-visualization-36387
3. Berger-Walliser, G., Barton, T.D., Haapio, H.: From visualization to legal design: A collaborative and creative process. Am. Bus. LJ **54**, 347 (2017)
4. Bernaerts, Y., Druwé, M., Steensels, S., Vermeulen, J., Schöning, J.: The office smartwatch: development and design of a smartwatch app to digitally augment interactions in an office environment. In: Proc. 2014 companion publication on Designing interactive systems, pp. 41–44 (2014)
5. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: The Next Generation Privacy Dashboard", booktitle="Privacy Technologies and Policy. pp. 135–152. Springer Int. (2016)
6. Billinghurst, M., Starner, T.: Wearable devices: new ways to manage information. Computer **32**(1), 57–64 (1999)
7. Burkhardt, D., Nazemi, K.: Visual legal analytics–A visual approach to analyze law-conflicts of e-Services for e-Mobility and transportation domain. Procedia Computer Science **149**, 515–524 (2019)

8. Conti, G.: Security data visualization: graphical techniques for network analysis. No Starch Press (2007)
9. Čyras, V., Lachmayer, F., Hoffmann, H., Weng, Y.H.: Introduction to Legal Visualization (2018)
10. Emami-Naeini, P., Agarwal, Y., Cranor, L.F., Hibshi, H.: Ask the Experts: What Should Be on an IoT Privacy and Security Label? (2020)
11. European Union: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). Official Journal of the European Union **L119**, 1–88 (2016)
12. Fabian, B., Ermakova, T., Lentz, T.: Large-Scale Readability Analysis of Privacy Policies. In: Proceedings of the International Conference on Web Intelligence. p. 18–25. WI '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3106426.3106427
13. Fan, X., Li, C., Dong, X.: A real-time network security visualization system based on incremental learning (ChinaVis 2018). Journal of Visualization **22**(1), 215–229 (2019)
14. Floridi, L.: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philos. Technol. **33**, 369—378 (2020)
15. Gabriele, S., Chiasson, S.: Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In: Proc. CHI Conference on Human Factors in Computing Systems. p. 1–12. CHI '20, ACM (2020)
16. Gerasimov, Arkadii and Michael, Judith and Netz, Lukas and Rumpe, Bernhard and Varga, Simon: Continuous transition from model-driven prototype to full-size real-world enterprise information systems. In: 25th Americas Conf. on Information Systems (AMCIS 2020). Association for Information Systems (AIS) (2020)
17. Haapio, H., Plewe, D., deRooy, R.: Next generation deal design: comics and visual platforms for contracting. In: Networks. Proc. 19th Int. Legal Informatics Symposium IRIS. pp. 373–380 (2016)
18. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A „Nutrition Label" for Privacy. In: 5th Symposium on Usable Privacy and Security. SOUPS '09, ACM (2009)
19. Koivisto, J., Hamari, J.: The rise of motivational information systems: A review of gamification research. Int. Journal of Information Management **45**, 191 – 210 (2019)
20. Kolter, J., Netter, M., Pernul, G.: Visualizing Past Personal Data Disclosures. In: Int. Conf. on Availability, Reliability and Security. pp. 131–139 (2010)
21. Kranich, L., Hauth, P., Pols, A.: Kompetenzen einer Digitalen Souveränität (11022020), `https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html`, Studie im Auftrag des BMWi
22. Lettieri, N., Altamura, A., Malandrino, D.: The legal macroscope: Experimenting with visual legal analytics. Information Visualization **16**(4), 332–345 (2017)
23. Mertz, M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C., Woopen, C.: Digitale Selbstbestimmung (2016), `https://kups.ub.uni-koeln.de/6891`, Technical Report
24. Michael, J., Netz, L., Rumpe, B., Varga, S.: Towards Privacy-Preserving IoT Systems Using Model Driven Engineering. In: Ferry, N., Cicchetti, A., Ciccozzi, F., Solberg, A., Wimmer, M., Wortmann, A. (eds.) Proc. of MODELS 2019. Workshop MDE4IoT. pp. 595–614. CEUR Workshop Proceedings (2019)

25. Michael, J., Steinberger, C.: Context Modeling for Active Assistance. In: Cabanillas, C., España, S., Farshidi, S. (eds.) ER Forum and Demo Track 2017 co-located with the 36th Int. Conf. on Conceptual Modelling (ER 2017). pp. 221–234 (2017)
26. Murmann, P., Fischer-Hübner, S.: Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access **5**, 22965–22991 (2017)
27. Nadeem, S.F., Huang, C.Y.: Data Visualization in Cybersecurity. In: Int. Conf. on Computational Science and Comp. Intelligence (CSCI). pp. 48–52. IEEE (2018)
28. Päßler, S., Wolff, M., Fischer, W.J.: Food Intake Recognition Conception for Wearable Devices. In: Proc. 1st ACM MobiHoc Workshop on Pervasive Wireless Healthcare. MobileHealth '11, ACM (2011)
29. Proctor, R.W., Ali, M.A., Vu, K.P.L.: Examining usability of web privacy policies. Intl. Journal of Human–Computer Interaction **24**(3), 307–328 (2008)
30. Schoormann, T., Hofer, J., Behrens, D., Knackstedt, R.: Rechtsvisualisierung in 20 Jahren IRIS–Eine multimethodische Literaturanalyse. In: Internationales Rechtsinformatik Symposium (IRIS). vol. 20 (2017)
31. Schoormann, T., Knackstedt, R., Haapio, H.: Modeling and Visualization in Law: Past, Present and Future. In: Int. Rechtsinformatik Symposium IRIS (2017)
32. Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A.: A survey of wearable devices and challenges. IEEE Communications Surveys & Tutorials **19**(4), 2573–2620 (2017)
33. Sethi, A., Wills, G.: Expert-interviews led analysis of EEVi—A model for effective visualization in cyber-security. In: IEEE Symposium on Visualization for Cyber Security (VizSec 17). pp. 1–8. IEEE (2017)
34. Stubbe, J., Schaat, S., Ehrenberg-Silies, S.: Digital souverän? Kompetenzen für ein selbstbestimmtes Leben im Alter. Bertelsmann Stiftung (2019)
35. Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., Shadbolt, N.: X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps. In: Proc. CHI Conference on Human Factors in Computing Systems. p. 1–13. CHI '18, ACM (2018)
36. Vermeulen, J., MacDonald, L., Schöning, J., Beale, R., Carpendale, S.: Heartefacts: augmenting mobile video sharing using wrist-worn heart rate sensors. In: Proc. ACM Conf. on Designing Interactive Systems. pp. 712–723 (2016)
37. Walser Kessel, C., Lachmayer, F., Čyras, V., Parycek, P., Weng, Y.H.: Rechtsvisualisierung als Vernetzung von Sprache und Bild – Anmerkungen zum Buch „Kennst Du das Recht?". In: Proc. of the 19th International Legal Informatics Symposium IRIS. pp. 365–371 (2016)
38. Weis, R., Lucks, S., Grassmuck, V.: Technologien für und wider Digitale Souveränität. Studien und Gutachten im Auftrag des Sachverständigenrat für Verbraucherfragen (SVRV) (2016)
39. Wenig, D., Schöning, J., Hecht, B., Malaka, R.: Stripemaps: Improving map-based pedestrian navigation for smartwatches. In: Int. Conf. on Human-Computer Interaction with Mobile Devices and Services. pp. 52–62 (2015)
40. Williams, L., Hayes, G.R., Guo, Y., Rahmani, A., Dutt, N.: HCI and MHealth Wearable Tech: A Multidisciplinary Research Challenge. In: Ext. Abstracts - CHI Conf. on Human Factors in Computing Systems. p. 1–7. CHI EA '20, ACM (2020)
41. Wittpahl, V.: Digitale Souveränität: Bürger, Unternehmen, Staat . Springer Viewег, Berlin, Heidelberg (2017)
42. Yan, T., Lu, Y., Zhang, N.: Privacy Disclosure from Wearable Devices. In: Workshop on Privacy-Aware Mobile Computing. p. 13–18. PAMCO '15, ACM (2015)
43. Yang, H., Yu, J., Zo, H., Choi, M.: User acceptance of wearable devices: An extended perspective of perceived value. Telematics and Informatics **33**(2) (2016)