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?

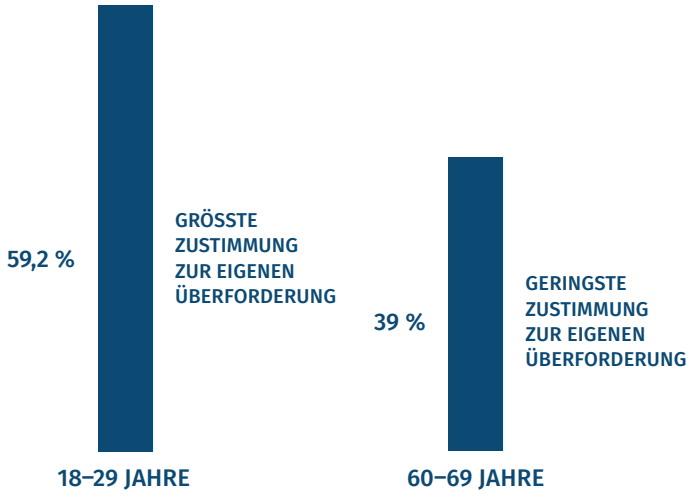
In der Tat: Datenschutzerklärungen oder -einstellungen, wie im Fall von Cookie-Bannern, bieten Nutzenden häufig keine oder nur umständliche Möglichkeiten, diese auf ihre Datenschutzbedürfnisse anzupassen. Das Ziel beim Design von User-Interfaces für Datenschutzerklärungen oder -einstellungen sollte daher 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.

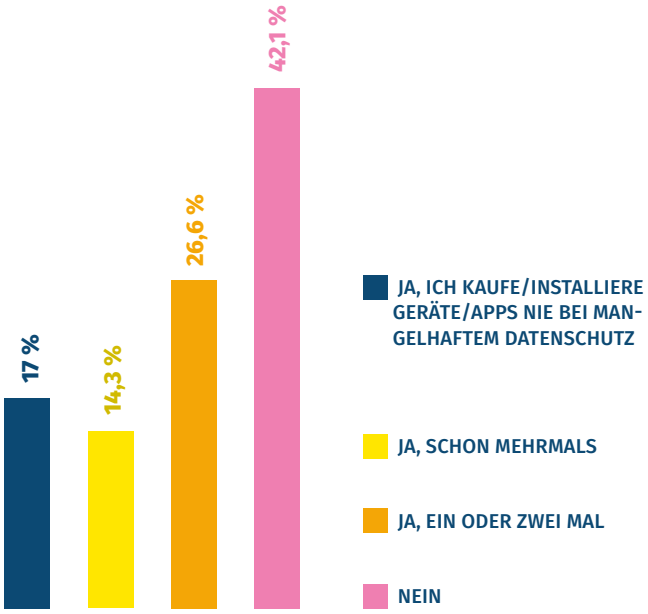
Ein weiteres Anwendungsgebiet ist der Bereich des Maschinellen Lernens. In diesem Bereich existiert zwar eine Reihe von mathematischen Ansätzen für den Datenschutz, aber deren Anwendbarkeit konnte bisher nur in wenigen praktischen Beispielen geprüft werden. Auch im Bereich des UX-Designs wird nutzer·innenorientiert 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.