Ausgabe 26

goo.gle/aufbruch-de

AUFBRUCH

Mensch und Gesellschaft im digitalen Wandel

Privatsphäre

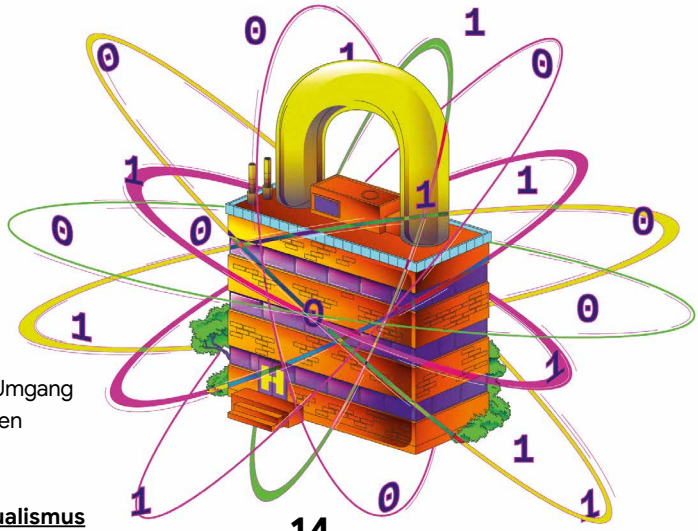
Sicher und geschützt: Wie aus anonymisierten Daten Innovation entsteht

Schnell und praktisch: Eine digitale Identität vereinfacht den Alltag

Made in München: So machen Googler:innen das Internet sicherer

Google

Inhalt



14

17

12

28

Cover: Ari Liloan (Illustration), Felix Brüggemann (Foto); Fotos: Lêmrich, Sima Dehgani, Matthias Oertel; Illustration: Ari Liloan; Foto Editorial: Google LLC

Impressum
Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland | Tel.: +353 1 543 1000 | Fax: +353 1 686 5660 | E-Mail: support-deutschland@google.com | Geschäftsführung: Elizabeth M. Cunningham, Nicholas Leeder | Google Ireland Limited ist eine nach irischem Recht gegründete und registrierte Gesellschaft | Registernummer: 368047 | Umsatzsteuer-ID.-Nr.: IE6388047V

Dies ist eine Anzeigensonderveröffentlichung von Google. Danke an das Team von SZ Scala GmbH.

Vorwort

Liebe Leserin, lieber Leser,

viele Menschen in Deutschland leben und organisieren mithilfe des Internets ihren Alltag. Sie planen Wege und Reisen, sie kaufen oder verkaufen, sie halten Kontakt zu Freunden oder tauschen sich in sozialen Netzwerken aus. Während die einen dabei auch Privates veröffentlichen, halten sich die anderen zurück. Die Grenzen der Privatsphäre verlaufen individuell ganz unterschiedlich.

Unabhängig davon, wie viel unsere Nutzer:innen teilen möchten: Wir entwickeln Google-Produkte immer so, dass alle Daten geschützt sind und die Privatsphäre jeder Einzelnen und jedes Einzelnen respektiert wird. Ein großer Teil dieser Arbeit geschieht in München, an einem unserer vier deutschen Standorte. Hier ist seit 2009 Googles weltweites Entwicklungszentrum für Datenschutz und Datensicherheit untergebracht: Mehrere Hundert Expert:innen aus der ganzen Welt arbeiten gemeinsam mit Partnern an einem besseren und sicheren Internet für alle.

Aus den Gesprächen mit unseren Nutzerinnen und Nutzern – unter anderem in München – wissen wir, wie wichtig gerade den Deutschen eine intakte digitale Privatsphäre ist; nur wer digitalen Anwendungen vertraut, verspürt die Motivation, mit ihrer Hilfe sein Leben und seine Arbeit zu gestalten. Dieses *Aufbruch*-Magazin zeigt, wie das Konzept der Privatsphäre entstand und wie es sich entwickelt; es möchte vermitteln, wie Wissenschaft, Politik und Unternehmen wie Google daran arbeiten, sie zu stärken.

Viel Freude beim Lesen!

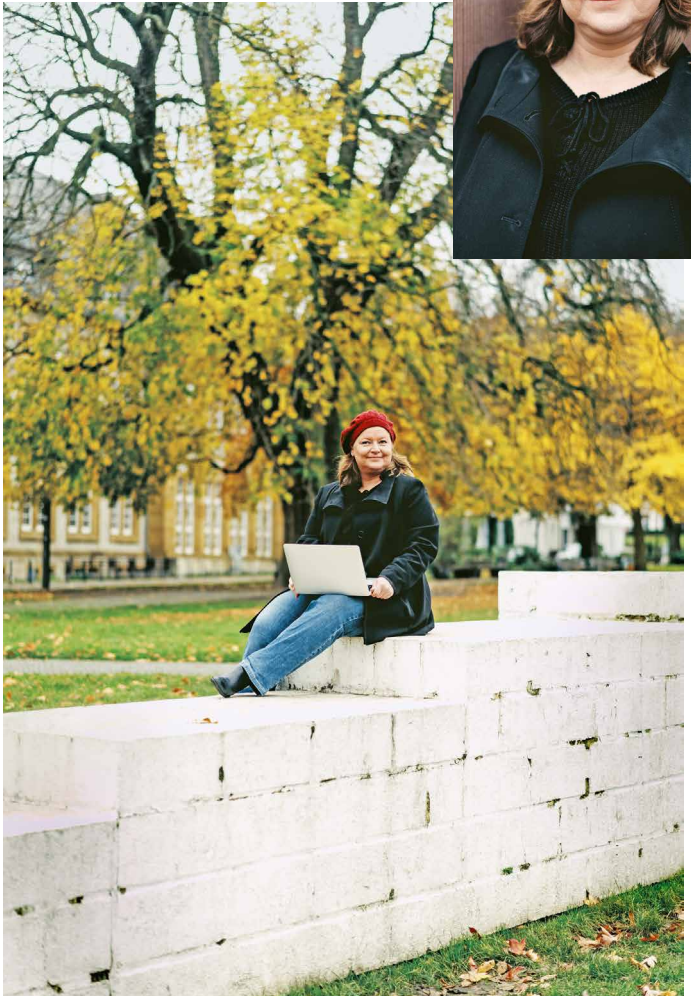
Ihr Philipp Justus
Vice President Google Zentraleuropa

Das *Aufbruch*-Magazin
In unserer Reihe zur Digitalisierung sind inzwischen 26 Ausgaben erschienen. Auf → *goo.gle/aufbruch-de* finden Sie alle Hefte zum Nachlesen.

Privatsache

Viele Menschen wägen täglich ab, was sie online teilen und was sie schützen. Sechs persönliche Geschichten über den Umgang mit Informationen in der Schule, im Internet oder in der Behörde

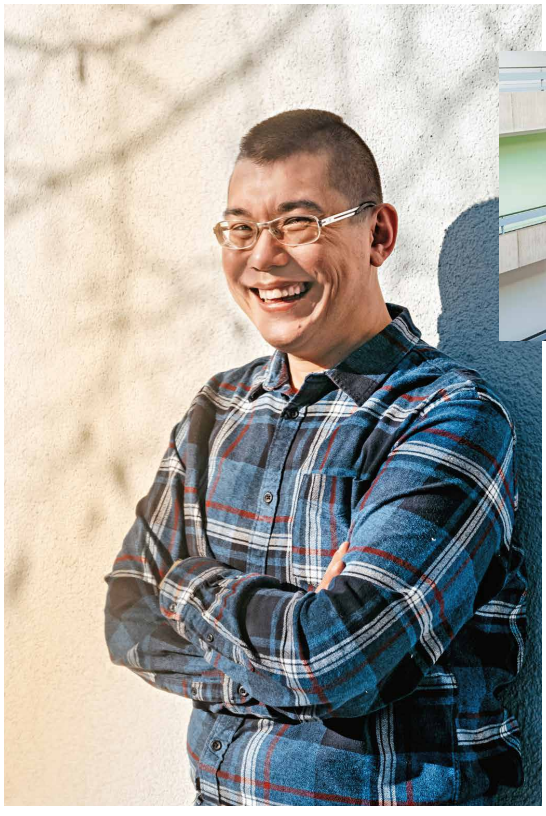
PROTOKOLLE: GRETA SIEBER
FOTOS: PATRICK SLESIONA, MARIA IRL, AXMANN–ROTTLER, FELIX BRÜGGEMANN, SIMA DEHGANI



»Ich achte darauf, welche Informationen von mir im Internet landen«

Susanne Holzgraefe arbeitet als Diplom-Informatikerin, Ingenieurin und zertifizierte Datenschutzbeauftragte in Bielefeld.
»Als ich ein Kind war, hat meine Mutter meinen Geschwistern und mir oft hinterhergeschnüffelt, etwa in der Schultasche. Wenn ich nicht wollte, dass sie etwas sieht, musste ich es gut verstecken. Privatsphäre ist mir seither unheimlich wichtig. Vielleicht habe ich mich deshalb für Datenschutz interessiert und mir neben meinem Beruf als Informatikerin und Ingenieurin dieses zweite Standbein aufgebaut. Einerseits berate ich Firmen in Sachen Datenschutz und schule Mitarbeitende zum Beispiel zum Thema Verschlüsselung. Andererseits decke ich als Datenschutzbeauftragte für Unternehmen Mängel auf. Zudem melden sich Menschen bei mir, wenn sie das Gefühl haben, ein Unternehmen geht mit ihren Daten nachlässig um.
Privat bin ich ebenfalls sehr achtsam. Einmal sind mir in der Umkleide eines Schwimmbads Kameras aufgefallen. Daraufhin habe ich den Datenschutzbeauftragten informiert. Ich achte auch genau darauf, welche Informationen und Fotos von mir im Internet landen. Dort finden sich keine nichtprofessionellen Fotos von mir oder Informationen darüber, ob ich Kinder habe. Das geht niemanden etwas an.«

»Füllen Bürger:innen Formulare aus, sind ihre Daten verschlüsselt«



Andreas Tang arbeitet als stellvertretender Leiter der IT im Landratsamt Straubing-Bogen.

»In unserer Behörde ist Datenschutz sowohl analog als auch digital wichtig. Das beginnt damit, dass wir sensible Dokumente nicht im normalen Papierkorb entsorgen, sondern im Aktenvernichter, oder dass es keine Arbeitsplätze gibt, die von außen einsehbar sind. Wenn wir Faxe erhalten, werden diese digitalisiert per Mail dem jeweiligen Sachgebiet zugestellt – das spart Papier, und die Daten liegen nicht für alle einsehbar im Faxgerät herum. Wenn Bürgerinnen und Bürger Formulare auf unserer Webseite ausfüllen, sind ihre Daten verschlüsselt.

Aktuell bilde ich mich zum IT-Sicherheitsbeauftragten weiter. Da muss ich die Mitarbeitenden für Datenschutz sensibilisieren: dass sie sichere Passwörter wählen – und diese nicht auf den Monitor kleben. Oder dass sie ihre Computer sperren, wenn sie ihren Arbeitsplatz verlassen. Am Ende kommt es auf das Verhalten jedes und jeder Einzelnen an. Außerhalb der Behörde rate ich dazu, sparsam mit den eigenen Daten umzugehen. Ich bin in keinem sozialen Netzwerk mit meinem echten Namen angemeldet.«

»Intime Momente würde ich nicht teilen«

Foto Isik: privat

YouTube-Creatorin Ischtar Isik beschäftigt sich mit Beauty- und Modethemen, ihr folgen mehr als eine Million Fans.

»Viele Fans folgen mir, seitdem ich auf YouTube aktiv bin – das ist seit 2011, dadurch entsteht schon eine Art Beziehung zur Community. Es fühlt sich an, als würde ich schöne und schwierige Momente mit Freundinnen und Freunden teilen. In den letzten Jahren waren das viele private Einblicke, zum Beispiel in meine Beziehung, das Zusammenziehen, die Verlobung, die Hochzeitsvorbereitungen. Ich versuche, eine gesunde Balance zu finden, indem ich zwar Persönliches teile, aber sensible Inhalte privat bleiben. Auf YouTube und Instagram zeige ich ja immer nur eine komprimierte Version meines Tages. Infos über bestimmte Familienmitglieder oder sehr intime Momente würde ich nicht teilen. Auch meine Wohngegend gebe ich nicht preis. Da ich auch selbst Videos schneide, kann ich entscheiden, was ich am Ende zeigen möchte. Zum Schutz meiner privaten Daten nutze ich zum Beispiel im Google-Konto die Zwei-Faktor-Authentifizierung, einen Identitätsnachweis, für den ich jeden Login zusätzlich auf einem meiner Geräte bestätigen muss.«

»Medienbildung muss auch im Privaten passieren«

Bob Blume ist Gymnasiallehrer für Englisch, Deutsch und Geschichte und bloggt auf bobblume.de über Bildung.

»Kinder und Jugendliche werden oft unterschätzt, was den Schutz ihrer Privatsphäre und Daten angeht. In Vertretungsstunden spreche ich gern mit Schülerinnen und Schülern über ihr Verhalten im Internet. Viele haben schon ein Bewusstsein dafür und nutzen zum Beispiel mehrere Social-Media-Accounts: einen, in dem sie öffentlich posten, und einen, in dem sie private Erfahrungen mit Freunden austauschen. In Baden-Württemberg wird in der fünften Klasse der Basiskurs Medienbildung angeboten, in dem die Kinder unter anderem lernen, was im Internet mit ihren Daten passiert.

Medienbildung muss aber auch im Privaten passieren. Familien sollten etwa offen darüber sprechen, wenn ein Kind merkwürdige Nachrichten von Fremden bekommt. Verbote aber bringen nicht viel. Wenn Jugendliche aufs Handy starren, sind sie nicht unbedingt Daddler – sie lesen, hören, schreiben mit den Geräten. Eltern sollten fragen, was sie machen, statt zu urteilen. Wenn wir Kinder und Jugendliche zu digitaler Mündigkeit erziehen wollen, müssen sie auch Geräte, Plattformen und Anwendungen nutzen können. Ich selbst teile vieles, was ich im und für den Unterricht tue, öffentlich, aber keine persönlichen Informationen aus Gesprächen oder direkten Interaktionen.«

»Ich lösche regelmäßig den Browserverlauf«

Dirk Hohnsträter leitet die Forschungsstelle Konsumkultur an der Universität Hildesheim und schrieb das Buch *Qualität! Von der Kunst, gut gemachte Dinge zu entdecken, klug zu wählen und genussvoll zu leben.*

»Beim Onlineshopping teilen wir einerseits absichtlich Daten, etwa Kontaktdetails für den Versand oder Informationen bei Kundenbefragungen und Produktrezensionen. Vieles gibt man aber auch unbewusst preis, wenn etwa eine Software unser Klickverhalten registriert. Auch in Werbemails wie Newslettern sind Tracker enthalten, die unter anderem auswerten, auf welche Links jemand klickt.

Für Unternehmen sind diese Informationen wertvoll, weil sie damit Werbung zielgruppengenau zuschneiden können. Teilweise nehmen die Menschen das auch positiv wahr. Aber niemand kann überschauen, wo welche Daten genutzt werden. Möglicherweise ist es ihnen nicht recht, wenn Unternehmen wissen, dass sie nach einem bestimmten Gesundheitsprodukt gesucht haben. Ich selbst ziehe den Browser weniger kontrollierbaren Einzel-Apps vor, lösche regelmäßig den Browserverlauf und nutze Plug-ins, die zum Beispiel das Abrufen von Standortdaten blockieren. Es gibt viele Möglichkeiten, um eine unerwünschte Datenpreisgabe abzuwehren.«

»Wir hatten Alleinzeiten, wenn eine von uns Besuch hatte«

Die Journalistin Katja Schwarz schrieb das Buch *How To Survive mit Geschwistern*.

»Privatsphäre in der Familie ist auf keinen Fall selbstverständlich. Ich musste mir lange ein Zimmer mit meiner Schwester teilen. Wir hatten je ein Hochbett, der Platz darunter war mit einem Vorhang als persönlicher Bereich abgetrennt. Außerdem hatten wir ›Alleinzeiten‹ im Zimmer, zum Beispiel wenn eine von uns Besuch hatte. Und jedes Familienmitglied hatte einen eigenen Zugang zum Computer mit individuellem Passwort. Heute bin ich selbst Mutter und finde, unsere Eltern haben uns gut vorgelebt, dass wir ein Recht auf Privatsphäre haben.

Zugleich merke ich, dass nicht alle dieselbe Definition davon haben. Für die eine ist das Smartphone tabu, für den anderen das Betreten des Badezimmers. Ich kommuniziere meine Grenzen direkt, auch innerhalb der Familie. Digital schütze ich meine Privatsphäre, indem ich nur die Pflichtfelder ausfülle, wenn ich persönliche Daten angeben muss. Und für unwichtige Vorgänge nutze ich eine andere Mail-Adresse als für wichtige – da kann dann auch Spam landen.«

Vom Kollektiv zum Individualismus

Dass Menschen »für sich« sein können, ist eine Errungenschaft der jüngeren Vergangenheit: Wie die Idee der Privatsphäre sich über die Jahrhunderte entwickelte und nun sogar zum europäischen Exportgut wird

TEXT: TATJANA KRIEGER; ILLUSTRATION: ARI LILOAN

Als Anfang September 1666 der Große Brand von London nach mehrtägigem Wüten endlich erloschen war, erkannten die Bewohner ihre Stadt nicht wieder: Im Zentrum waren 80 Prozent der Gebäude zerstört, zahlreiche mittelalterliche Bauten unwiederbringlich verloren. Dass nach offiziellen Angaben nur neun Menschenleben zu beklagen waren, erschien wie ein Wunder. Tatkräftig machte sich das Bürgertum an den Wiederaufbau seiner Häuser und Wohnstätten. Aber das London, das sich aus der Asche erhob, war ein anderes: Zwischen Häusern und Bordstein waren Freiräume entstanden. Türschwellen und Klingeln hielten den öffentlichen Raum auf Distanz. Das öffentliche Leben war etwas, das die Menschen mit Sünde, Verbrechen und Krankheiten assoziierten. Wer es sich leisten konnte, zog sich etwas zurück. Der Historiker Christoph Heyl wertet dieses Ereignis als den Ursprung des Privatsphäre-Begriffs in der westlichen Welt. Das Bürgertum mit seinen aufkommenden Wünschen nach Abgeschiedenheit und privaten Beschäftigungen wie Lesen oder dem Führen eines Tagebuchs trug demnach aktiv zur Verbreitung dieser damals noch neuen Idee bei.

»In der Antike gab es wenig Intimität«

Diese Form des Rückzugs war zuvor über Jahrtausende kaum ein Thema gewesen. »In der Antike gab es relativ wenig Intimität«, sagt der Historiker Wolfgang Schmale, der lange am Institut für Geschichte der Universität Wien gelehrt hat. Das Leben spielte sich oftmals im Freien ab, unter den Augen und der sozialen Kontrolle von Nachbarn und anderen Sittenwächtern. »Eine frühe Form der Unverletzlichkeit der Wohnung etablierte sich erst im Mittelalter, spätestens ab der Renaissance.«

Von da an hing es unter anderem von den Ressourcen ab, wie viel Privatheit sich Menschen leisten konnten. Persönliche Informationen oder gar Daten im heutigen Sinne standen noch nicht im Fokus; zunächst zählten vor allem physische und räumliche Privatsphäre. Diese wiederum bezog sich nach und nach nicht mehr nur auf die äußere Welt, denn auch im Inneren der Häuser änderte sich etwas: Es entstanden räumlich getrennte Schlafräume für Bewohner und Personal, Kinder bekamen ihr eigenes Zimmer – ganz anders als bei den mittellosen Arbeitern, die noch im frühen 20. Jahrhundert in Gruppen auf engstem Raum lebten und schliefen.

Jeder Personenkreis besitzt eine eigene Art der Privatsphäre

»Das Bedürfnis nach mehr Raum geht einher mit der zunehmenden Betonung des Individualismus«, analysiert Wolfgang Schmale. Wohlhabende Bauern mit großen Häusern gab es etwa schon immer. »Ein eigenes Zimmer hatten die Kinder trotzdem selten. Die allgemeine Vorstellung, wie eine Familie zu leben habe, stand dem entgegen.« Denn Gemeinschaftlichkeit und Nähe statt Individualismus und Persönlichkeitsentfaltung waren lange das vorherrschende Ideal. Das änderte sich im vergangenen Jahrhundert, und das Bedürfnis nach mehr Raum und nach mehr Privatheit wächst bis heute. Während die oder der Durchschnittsdeutsche im Jahr 2000 noch auf 39,5 Quadratmetern lebte, betrug die durchschnittliche Wohnfläche im Jahr 2020 schon 47,4 Quadratmeter – ein Anstieg um stolze 20 Prozent.

Seit den ersten Bemühungen um Privatheit hat sich der Anspruch an die Privatsphäre stetig gewandelt. In der Gegenwart verbinden die meisten Menschen mit dem Begriff sehr konkrete Dinge: Manche denken an einen Ort, an dem sie unbeobachtet und unbelauscht bleiben, andere denken an ein Geheimnis, das die Vertrauensperson nicht weitererzählt – oder an persönliche Daten, die verschlüsselt und passwortgeschützt sind.

»Das Verständnis von Privatsphäre hängt von ihrem Gegenteil ab: dem öffentlichen Raum«, erklärt Georg Kamphausen von der Kulturwissenschaftlichen Fakultät der Universität Bayreuth. »Privatheit schließt andere zunächst aus.« Wir leben heute in Personenkreisen. Mal bewegen wir uns im Kreis der Arbeits-

kolleg:innen, mal im Sportverein, mal in einer politischen oder kirchlichen Gemeinde. Jeder Personenkreis besitzt eine eigene Art der Privatsphäre mit spezifischen Themen und Tabus. Weil diese einst verbindlichen sozialen Bindungen heute an Bedeutung verlieren, sei es, so Kamphausen, immer schwieriger zu bestimmen, was privat sei und was nicht.

In Deutschland wurde die Frage nach den Grenzen der Privatheit an mehreren Stellen vehement diskutiert. Jeanette Hofmann ist Professorin für Internetpolitik und forscht an der Freien Universität Berlin am Wissenschaftszentrum Berlin für Sozialforschung zu Global Governance, Regulierung des Internets und Digitalem Wandel. Sie sagt: »Die Idee persönliche Daten aktiv zu schützen, kam in Deutschland erst in den 1970er-Jahren auf, nämlich mit der Ausbreitung der Großcomputer.« Damals stellte sich angesichts der neuen technologischen Möglichkeiten zum Sammeln, Speichern und Verarbeiten von Daten ein erstes Unbehagen ein.

Eine nächste Welle rollte über Deutschland, als der Staat für das Jahr 1981 eine Volkszählung ankündigte. Der von einem breiten gesellschaftlichen Bündnis getragene Protest gegen die Erfassung von persönlichen Daten führte schließlich zum Volkszählungsurteil und zum Grundrecht auf informationelle Selbstbestimmung. Die Volkszählung wurde erst sechs Jahre später durchgeführt als geplant. »Was damals geschah, war sehr spezifisch deutsch«, sagt Hofmann. »Der Wunsch nach informationeller Selbstbestimmung ist unter anderem den Erfahrungen im Nationalsozialismus geschuldet.« Im Lauf des Zweiten Weltkriegs, in einer Zeit der Diktatur und Überwachung, wurde den Menschen in Deutschland bewusst, welche Auswirkungen es haben kann, wenn der Staat Personendaten sammelt und für seine Absichten verwendet.

Diese Verunsicherung hallt noch heute nach, auch in den Debatten um Datenschutz im Internet: Wer sieht, welche Seiten ich online angesteuert habe? Kann jemand meinen Kontostand beim Onlinebanking mitlesen? Während sich sensible Informationen wie Bankgeschäfte jedoch nur auf kriminelle Weise ausspähen lassen, hinterlassen andere digitale Aktivitäten, über die viele gar nicht nachdenken, durchaus Spuren. »Es ist ein Paradox, dass wir durch unser Verhalten jeden Tag Daten produzieren, aber das Datensammeln ablehnen«, sagt der Historiker Wolfgang Schmale.

»Ohne den Schutz der Privatsphäre kann es keine Demokratie geben«

Die Perspektive der Menschen auf Privatheit im Internet ist heute denkbar divers. Während manche kategorisch darauf verzichten, persönliche Daten weiterzugeben, sind Anhänger der Post-Privacy-Idee (»Nach der Privatheit«) bereit, die Kontrolle komplett abzugeben. Ihnen zufolge bewegen wir uns auf einen Gesellschaftszustand zu, in dem weder Privatsphäre noch Datenschutz eine Rolle spielen werden. Jeanette Hofmann hält diesen Fatalismus für gefährlich. »Ohne den Schutz der Privatsphäre kann es keine Demokratie geben«, sagt die Wissenschaftlerin. »Es gehört zur Meinungsfreiheit, dass jeder Mensch selbst darüber entscheiden kann, was für Dritte sichtbar wird und was unsichtbar bleibt. Das gilt vor allem auch für die politische Meinung.«

Hofmann beobachtet, dass das Ringen um den Datenschutz ein europäisches, wenn nicht sogar deutsches Phänomen ist. »Ich stelle erhebliche Unterschiede in der Gewichtung von Grundrechten fest«, sagt sie. »In den USA ist das Recht auf freie Meinungsäußerung absolut sakrosankt. Mit dem europäischen Datenschutz tut man sich aber schwer.« Ähnlich sei es in den asiatischen Ländern. In der Europäischen Union sind sowohl das Recht auf Privatsphäre als auch der Datenschutz in der Charta der Grundrechte verankert. Daraus leitet sich ein starkes Schutzniveau ab. »Die Europäische Union ist in dieser Hinsicht am fortschrittlichsten«, findet auch Jeanette Hofmann. So fortschrittlich, dass die vergleichsweise junge EU-Datenschutz-Grundverordnung (DSGVO) auch in Asien und anderen Teilen der Welt bereits Standards gesetzt hat. •

»Der Datenschutz hat Zähne bekommen«

Jan Philipp Albrecht war maßgeblich an der Entstehung der EU-Datenschutz-Grundverordnung (DSGVO) beteiligt, die 2018 in Kraft trat. Heute ist er als Minister in Schleswig-Holstein für Digitalisierung zuständig. Im Interview erzählt Albrecht, wie er inzwischen auf das Regelwerk blickt und warum er die DSGVO für innovationsfördernd hält

INTERVIEW: SINAH HOFFMANN, FOTOS: MATTHIAS OERTEL

Herr Albrecht, Sie werden oft als »Vater der DSGVO« bezeichnet. Was löst das in Ihnen aus?
Ich freue mich darüber. Es ist ja tatsächlich so, dass ich als Berichterstatter des Europäischen Parlaments in einer ganz zentralen Funktion an der Verabschiedung des Gesetzes beteiligt war.

Was genau waren Ihre Aufgaben?
Ich war sozusagen Verhandlungsführer und Koordinator für die Ausarbeitung der Datenschutz-Grundverordnung. In meiner Verantwortung lag es, die Positionen innerhalb des Parlaments auszuhandeln, sie in einem Bericht zu bündeln und diesen dann mit dem Ministerrat abzustimmen. Insgesamt zog sich der Prozess über sieben Jahre.

Auch weil sich einige EU-Staaten lange gegen die Verordnung stellten. Einen Ihrer ersten Gesetzentwürfe überzogen die Abgeordneten mit über 4000 Änderungswünschen. Am Ende konnten Sie das Parlament dennoch überzeugen. Sind Sie zufrieden dem Ergebnis?
Absolut. Wir haben mit der Einführung der DSGVO auf europäischer Ebene etwas erreicht, was in anderen Bereichen noch nicht so gut funktioniert. Nämlich ein einheitliches und EU-weites Regelwerk zu verankern, das die Rechte Einzelner bei der digitalen Verarbeitung ihrer Daten schützt – auch gegenüber ausländischen Firmen. Darauf können wir stolz sein.

Was ist aus Ihrer Sicht die größte Errungenschaft der DSGVO?
Die Transparenz und die Selbstbestimmung der Bürgerinnen und Bürger. Unternehmen müssen jetzt viel umfangreicher informieren und explizit um Einwilligung bitten, wenn sie personenbezogene Daten weiterverarbeiten – und auch erklären, wie und zu welchem Zweck sie das tun.

» Wer die Rahmenbedingungen erfüllt, hat sogar einen Vorsprung auf dem Weltmarkt «

Gleichzeitig sind die Firmen verpflichtet, die persönlichen Daten wieder zu löschen, wenn kein Verarbeitungsgrund mehr gegeben ist. Was aber auch gesagt werden muss: Die Datenschutz-Grundverordnung ist keine neue Erfindung und auch keine Revolution. Viele Prinzipien, die in ihr verankert sind, gelten bereits in ähnlicher Form seit den 90er-Jahren.

Warum wurden sie nicht umgesetzt?
Weil die Gesetze sehr vage formuliert waren. Die verschiedenen EU-Staaten haben sie unterschiedlich ausgelegt, besonders wenn es darum ging, Unternehmen klare Grenzen aufzuzeigen. Das hat dazu geführt, dass Firmen ihre Standorte in Länder mit freundlicheren Regeln verlegten. Das ist mit der DSGVO nicht mehr so einfach. Der Datenschutz hat Zähne bekommen. Es gibt jetzt nicht nur einheitliche Regeln, sondern auch einheitliche Sanktionen, wenn sich Firmen nicht an sie halten.

Welche Konsequenzen drohen ganz konkret?
Wenn ein Unternehmen nicht die Bedingungen zur Datenverarbeitung erfüllt, kann das bis zu vier Prozent seines weltweiten Umsatzes oder bis zu 20 Millionen Euro Strafe bedeuten. Das sind Summen, die selbst große Konzerne nicht einfach aus der Portokasse zahlen. Das führt dazu, dass viele Firmen Datenschutz längst nicht mehr nur als »nice to have« betrachten, sondern ihn ins Zentrum ihrer Unternehmungen stellen. Die DSGVO gilt im Übrigen auch für Datenverarbeiter außerhalb der EU, sofern sie ihre Dienste auf dem europäischen Binnenmarkt anbieten. Dieses Marktortprinzip stellt sicher, dass die europäischen Online-Unternehmen denselben Regeln unterliegen wie ihre ausländischen Konkurrenten – zum Beispiel aus dem Silicon Valley.

Neben hohen Strafen beklagen Unternehmen oft die mit der DSGVO verbundene Bürokratie. Ist die Verordnung nicht doch ein Innovationskiller?
Ganz im Gegenteil. Die Akzeptanz und das Vertrauen der Menschen gegenüber neuen

Zur Person

Jan Philipp Albrecht ist seit September 2018 Minister für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung in Schleswig-Holstein. Zuvor war der Grünen-Politiker neun Jahre lang Mitglied des Europaparlaments. Dort trieb der Jurist als zuständiger Berichterstatter die Entwicklung der europäischen Datenschutz-Grundverordnung maßgeblich voran.

Technologien haben über Jahre stark abgenommen. Auch weil nicht sicher war, wie weit die eigene Privatsphäre im Netz geschützt ist. Die DSGVO kann das jetzt ändern und schafft überhaupt erst die Voraussetzung dafür, Innovationen wieder zügiger voranzutreiben.

Inwiefern?

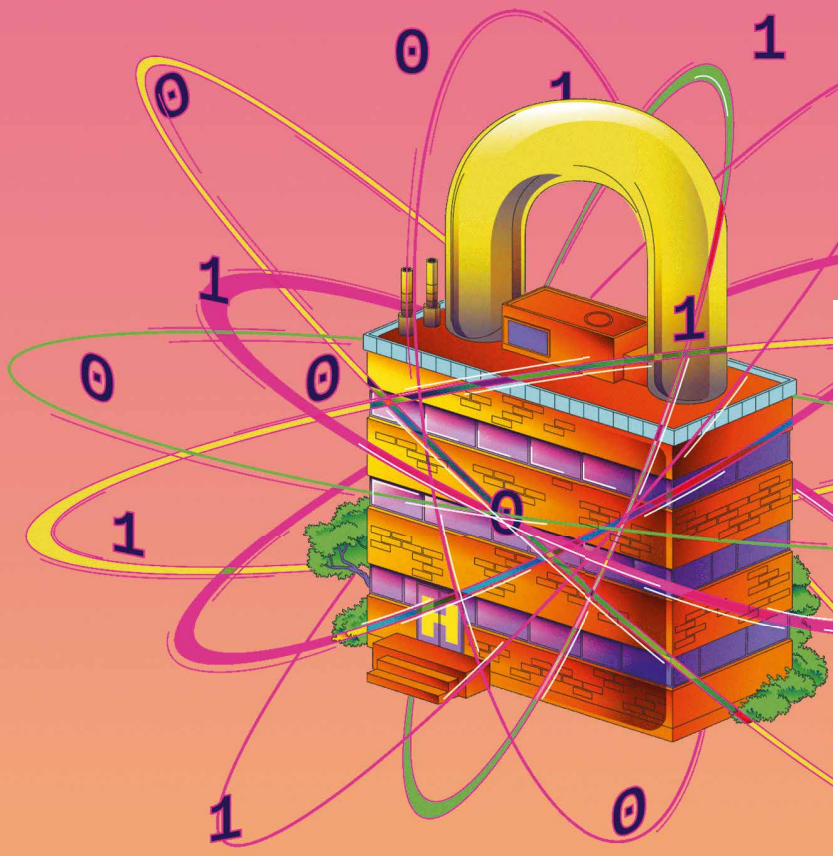
Das Regelwerk verbietet nicht die Datenverarbeitung, sondern definiert lediglich die Rahmenbedingungen. Wer diese erfüllt, hat sogar einen Vorsprung auf dem Weltmarkt. Ich glaube, viele Menschen unterschätzen, welchen großen Einfluss die DSGVO auf die Einführung internationaler Standards hat. Länder wie Japan und einige Bundesstaaten in den USA nutzen sie bereits als Schablone für eigene Gesetze. Wir übernehmen mittlerweile digitale Führungsverantwortung – und verschaffen uns damit einen wirtschaftlichen Wettbewerbsvorteil. Datenschutzfreundliche Technologien und Software made in Europe sind global sehr begehrt.

Sie sind seit 2018 der Digitalminister Schleswig-Holsteins. Wie schützen Sie Ihre Daten im Netz?

Ich versuche dort, wo es nicht zwingend notwendig ist, auf die Freigabe meiner persönlichen Informationen zu verzichten. Denn es gibt im Internet nach wie vor ein erhöhtes Risiko, dass die Daten irgendwo landen, wo sie nicht hingehören.

Braucht der Schutz der Privatsphäre zeitnah ein Update, eine Weiterentwicklung?

Im Moment liegt der Fokus auf Umsetzung und Durchsetzung der DSGVO. Die Regeln sind zukunftssicher und technikneutral formuliert. Im Bereich der künstlichen Intelligenz sind ein paar Anpassungen sicherlich sinnvoll, zum Beispiel beim Umgang mit verhaltensbasierter Werbung. In der Diskussion wird es darum gehen müssen, wo wir moralische und ethische Grenzen setzen – auch jenseits des Datenschutzes. •



Sicheres Geschäft

Digitalisierung geht nicht ohne Datenschutz. Das erkennen auch immer mehr Gründerinnen und Gründer, die sich auf Privatsphäre konzentrieren. Vier deutsche Start-ups und ihre Ideen zwischen Anonymisierung und Aufklärung

TEXTE: SINAH HOFFMANN, ILLUSTRATIONEN: ARI LILOAN

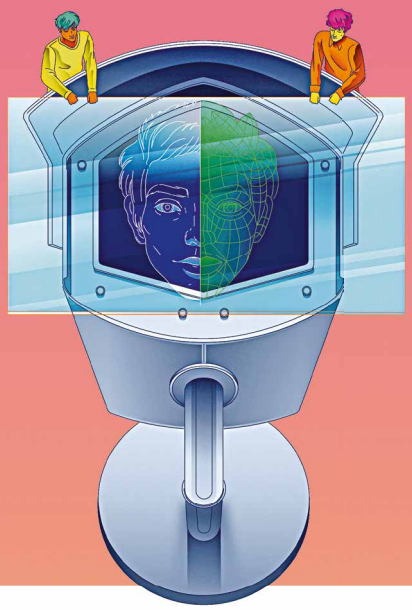
Wie Medizin auch mit anonymisierten Daten besser wird

Von der Prävention durch digitale Apps bis hin zu personalisierten Krebstherapien – der Einsatz von künstlicher Intelligenz (KI) in der Medizin könnte vielen Menschen nachhaltig helfen. KI-Systeme sind bei ihrem Lernprozess allerdings auf möglichst große und diverse Datensätze angewiesen. Je mehr Informationen sie bekommen, desto besser können sie Muster und Gesetzmäßigkeiten erkennen und berechnen – zum Beispiel wie verschiedene Medikamente aufeinander reagieren. Aber gerade Patient:innendaten sind sehr sensibel und dürfen nicht einfach mit anderen geteilt werden. »Krankenhäuser und Forschende müssen darum oft mit ihren eigenen kleinen Datensätzen arbeiten – und die sind meistens nicht aussagekräftig«, erklärt Robin Röhm, Mitgründer des Berliner Start-ups Apheris. Um das zu ändern, haben er und sein Team eine Technologie entwickelt, dank der die verschiedenen Parteien keine persönlichen Informationen, sondern nur anonyme Ergebnisse miteinander teilen.

Vereinfacht gesagt funktioniert das so: Forschende sammeln die Daten nicht an einem zentralen Ort, sondern senden über die Apheris-Plattform eine Rechenanfrage an die jeweilige Institution, zum Beispiel ein Krankenhaus. Die sensiblen Daten verlassen dann nicht ihre Umgebung, sondern werden vor Ort bei ihrem Eigentümer von der Software analysiert und berechnet. Am Ende kommt nur das Ergebnis, zum Beispiel in Form einer Statistik, verschlüsselt zurück und wird dem Algorithmus zusammen mit den anonymisierten Erkenntnissen anderer Institutionen zum Lernen zugespielt. Die Identität der Patientinnen und Patienten in dem jeweiligen Datentopf lässt sich so unmöglich zurückverfolgen.

Das Problem der Datensilos will Apheris aber nicht nur im Gesundheitswesen lösen. »Auch in anderen Bereichen, in denen Datenschutz eine große Rolle spielt, können Akteure dank unserer Technologie miteinander kollaborieren. Zum Beispiel wenn es darum geht, Lieferketten nachhaltiger zu organisieren«, verspricht Röhm. Die Jury des Bundesministeriums für Wirtschaft und Energie wählte das Unternehmen unter anderem wegen seiner branchenübergreifenden Lösung zum »Digitalen Start-up des Jahres 2020«.

→ *apheris.com*



Die Software macht Gesichter im öffentlichen Raum unkenntlich

Mit Computerhilfe lässt sich das Leben an vielen Stellen besser organisieren. Die Aufnahmen einer Kamera vom Straßenverkehr oder von Besucherbewegungen, etwa bei einer Großveranstaltung, kann ein Computerprogramm mithilfe künstlicher Intelligenz analysieren. Die Verantwortlichen können die Erkenntnisse dann für eine bessere Koordination der Fahrzeug- oder Menschenströme nutzen. Nur gibt es da ein Problem: Über eine automatisierte Gesichtserkennung könnte die Identität einzelner Personen aus den Aufnahmen herausgefiltert und so persönliche Bewegungsprofile und Verhaltensmuster erkennbar werden. »Überall, wo in der Öffentlichkeit Kameras zum Einsatz kommen, ist der Datenschutz ein großes Thema«, sagt Marian Gläser, Mitgründer des Start-ups »brighter AI«. Das junge Unternehmen entwickelte eine Technologie, die Gesichter und Nummernschilder in Videoaufnahmen anonymisiert.

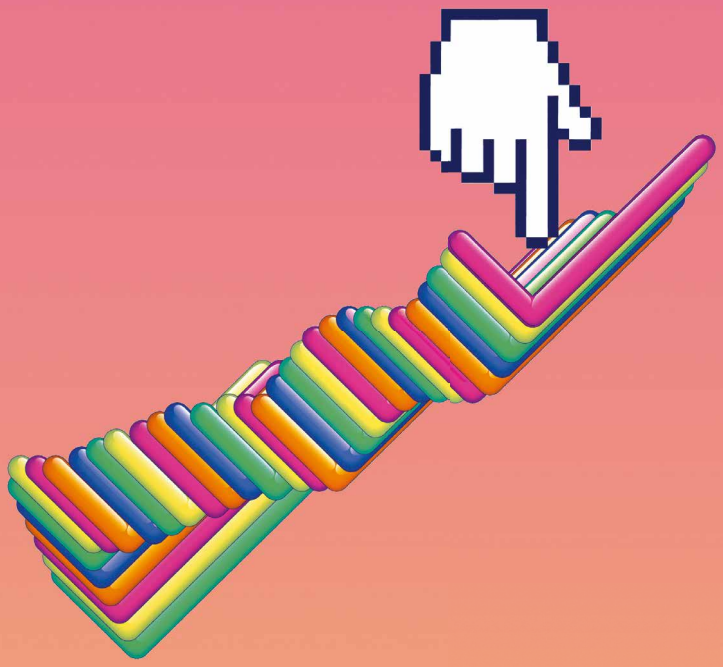
Dafür werden die Kameradaten auf den Servern der Unternehmenskunden oder in der Cloud durch eine Software geschleust. Die sogenannte Deep Natural Anonymization erkennt automatisch personenbezogene Informationen und generiert synthetische Nachbildungen mit den gleichen Attributen wie Geschlecht, Alter und Mimik. »Das Gesicht ähnelt danach sehr stark dem Original, kann aber nicht mehr identifiziert werden. So schützen wir die persönliche Identität und erhalten gleichzeitig wichtige Parameter, mit denen ein Algorithmus arbeiten kann«, erklärt Gläser. Zum Einsatz kommt die Technologie von brighter AI aktuell bei einem Pilotprojekt der Deutschen Bahn. In ausgewählten Zügen hilft eine intelligente Videoanalyse in Echtzeit dabei, die Passagiere in den Zügen besser zu verteilen und Corona-Abstandsregeln einzuhalten. → *brighter.ai*

Ein Programm vermittelt praxisnah Datenschutzwissen

Die Datenschutz-Grundverordnung ist komplex und durchdringt nahezu jeden Bereich eines Unternehmens. Während große Firmen und Konzerne in der Regel eigene Rechtsabteilungen beschäftigen, sind kleine und mittelständische Betriebe oft auf sich allein gestellt – und damit überfordert. »Keiner weiß so richtig, wo Datenschutz anfängt und wieder aufhört«, sagt Alexander Ingelheim, Co-Gründer des Start-ups datenschutzexperte.de. Zusammen mit Dominik Fünkner hat er darum eine Software programmiert, die wie ein digitaler Anwalt funktioniert.

Wollen Mitarbeitende etwa Dankeskarten an ihre Kundschaft verschicken, stellt das Tool detaillierte Fragen. Zum Beispiel, wo die Adressen herkommen und ob die Kund:innen schriftlich der Weiterverarbeitung ihrer Daten zugestimmt haben. Anhand der Antworten erkennt das Programm automatisch, ob der Datenschutz gewahrt wird, wo Probleme auftauchen und wie sie sich ganz konkret lösen lassen. »Die Software nimmt die Firmen an die Hand und führt sie Schritt für Schritt durch das Thema. So lernen auch Mitarbeitende ohne Vorkenntnisse nach und nach, worauf es beim Datenschutz ankommt«, erklärt Ingelheim. Für neue oder komplexe Fälle, die nicht in der Software definiert sind, stellt das Start-up zusätzlich Datenschutzexperten bereit, die sich persönlich um eine Lösung kümmern.

Gegründet wurde das Legal-Tech-Unternehmen 2017 in München. Mittlerweile betreuen über 70 Mitarbeiter:innen mehr als 1500 Firmen in ganz Deutschland. Für die Zukunft haben Ingelheim und sein Team bereits eine neue Vision: »Wir wollen auch für andere rechtliche Regelwerke einfache und verständliche Fragenkataloge erstellen. Ein großes Thema in der nächsten Zeit wird das Lieferkettengesetz sein.«
→ *datenschutzexperte.de*



Initiative Google for Startups

Wie baue ich eine App, die nicht nur cool und nützlich ist, sondern auch die Privatsphäre meiner potenziellen Nutzer:innen optimal respektiert? Datenschutz ist für praktisch jedes Start-up relevant, auch wenn sein Kernprodukt etwas ganz anderes ist. Neben vielen weiteren Themen, die für Gründer:innen wichtig sind, bietet die Initiative Google for Startups auch Unterstützung, Trainings und Informationen rund um den Schutz von Kundendaten.
→ startup.google.com

In Zusammenarbeit mit Expert:innen des Google Safety Engineering Centers in München werden Workshops, Schulungen und Austausch zu den Themen Datenanonymisierung und User Experience Design mit dem Fokus auf den Schutz von Privatsphäre angeboten.
→ goo.gle/gsec

Wie Unternehmen ihr »Consent Management« vereinfachen können

Sie ploppen auf, sobald man eine Webseite öffnet: Cookie-Banner. Unternehmen sind per Gesetz verpflichtet, Nutzer:innen darüber zu informieren, wenn sie bestimmte Web-Technologien verwenden, die personenbezogene Daten an Dritte verkaufen oder weiterverarbeiten. Zum Beispiel um anhand des Verhaltens im Netz ein Profil zu erstellen, zu dem auch Einschätzungen zur Einkommensklasse und sogar zum IQ zählen können. Die Endkund:innen haben nicht nur ein Recht darauf zu erfahren, wohin ihre Daten fließen, sondern müssen unter Umständen auch zustimmen, dass diese im Internet überhaupt nachverfolgt werden dürfen.

Webseitenbetreibende stellt das vor große technische und administrative Herausforderungen. Unterstützung verspricht das Start-up Usercentrics. »Unsere Software hilft Unternehmen dabei, Einwilligungen – aktuell sind es etwa 60 Millionen pro Tag – datenschutzkonform über alle digitalen Kanäle hinweg einzuholen, zu verwalten und zu dokumentieren«, erklärt Gründer Mischa Rürup.

Mithilfe der »Consent Management«-Lösungen können Unternehmen selbst entscheiden, welche Art von Privacy-Banner sie einsetzen möchten, auf welcher Rechtsgrundlage die einzelnen Dienste Daten erheben – und ob es einen »Ablehnen«-Button geben soll oder nicht. »Wir helfen den Werbetreibenden bei der Einwilligung, versuchen aber gleichzeitig, die Banner möglichst transparent zu gestalten, und raten unseren Kund:innen dazu, die ›Zulassen‹- und ›Ablehnen‹-Buttons gleichberechtigt nebeneinander zu platzieren«, erläutert Rürup.

Genutzt wird die Technologie mittlerweile von Unternehmen wie Audi, Porsche und der Deutschen Bank. Nun will Usercentrics sie auch international exportieren. »Nur etwa 15 bis 20 Prozent der Menschen weltweit sind bislang durch Gesetze in ihrer Privatsphäre geschützt. Das wird sich aber bald ändern. Länder wie Brasilien und Japan nehmen bereits jetzt die europäische Datenschutz-Grundverordnung als Schablone für ihr eigenes Regelwerk. Datenschutz ist ein Zukunftsmarkt«, so Rürup.
→ usercentrics.com

Das digitale Ich in einer Hand

Mithilfe digitaler Identitäten könnten Bürger:innen bald per Smartphone nachweisen, wer sie sind – aber auch, welchen Bildungsabschluss, Beruf, Grundbesitz oder Ehestand sie haben. Die neuen Möglichkeiten sollen den Alltag erleichtern und den Schutz der eigenen Identitätsmerkmale stärken

TEXT: CHRISTOPH HENN
FOTOS: LÊMRICH, FELIX ADLER

Wenn Jürgen Anke, Professor für Softwaretechnologie und Informationssysteme an der HTW Dresden, der Kita seines Sohnes etwas mitteilen möchte, ist das manchmal ein aufwendiger Prozess. Sollen andere Eltern den Kleinen direkt von der Kita zu einer Geburtstagsfeier mitnehmen, benötigen sie eine Abholberechtigung. »Diese Information ist wichtig, und die Kita muss sich darauf verlassen können, dass sie zweifelsfrei von mir stammt«, so Jürgen Anke. Streng genommen muss der Vater dafür ein Formular ausfüllen, es unterschreiben und eindeutig nachweisen, dass die Mitteilung tatsächlich von ihm oder seiner Frau kommt. Ähnlich ist es bei vielen anderen typischen Einzelregelungen in Kitas, die sensible Themen betreffen, etwa bei Informationen zu Lebensmittelallergien.

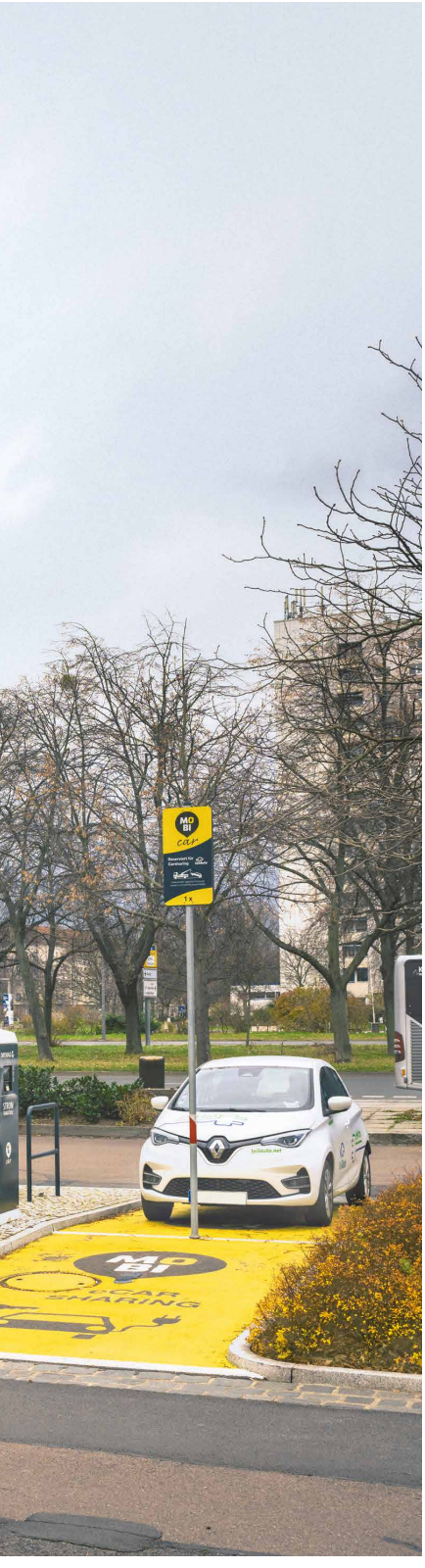
Wenn es nach dem Dresdner geht, laufen solche Kita-Prozesse bald komplett digital ab, denn eines von Jürgen Ankes Spezialgebieten sind digitale Identitäten. »Viele verbinden mit Identität vor allem Name, Geburtsdatum, Wohnort«, sagt er, »aber zur Identität jeder und jedes Einzelnen gehören viel mehr Merkmale, als im Personalausweis stehen.« Mit vielen anderen arbeitet der Wissenschaftler daran, dass künftig digitale Nachweise all jene Facetten einer Identität belegen, für die bislang zahllose Ausweise und Zertifikate aus Papier oder Plastik existieren: Schülerausweise, Hochschulzeugnisse, Schwerbehindertenausweise, Stadtpässe für sozial Benachteiligte, Grundbuchauszüge für Immobilienbesitzer:innen, Trauscheine für Verheiratete und so weiter.

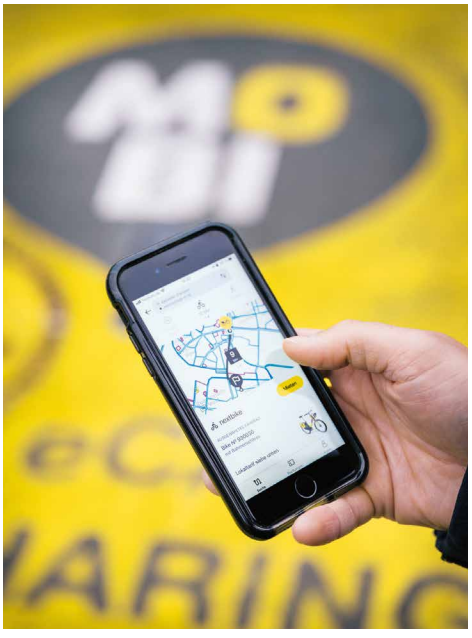
Um zu erforschen, wie sich Identitätsmerkmale im Alltag nachweisen lassen, wurde in Sachsen »ID-Ideal« ins Leben gerufen. Dabei testen Wissenschaft, Behörden und Unternehmen gemeinsam, wie digitale Identitäten in unterschiedlichsten Lebensbereichen genutzt werden können. Das Kita-Szenario, bei dem Eltern rechtsverbindliche Meldungen übermitteln können, ist nur einer von mehreren Anwendungsfällen. Ein anderes Szenario dreht sich um Mobilität: »Wir wollen erreichen, dass sich in Dresden und Leipzig mit einem digitalen Fahrausweis alle Verkehrsmittel nutzen lassen, von Bussen und Bahnen bis hin zu Leihrädern, E-Scootern und Car-Sharing«, sagt Anke.

Nur die nötigsten Merkmale übertragen

Damit das funktioniert, will ID-Ideal alle notwendigen Nachweise wie persönliche Daten, Zahlungsinformationen, Ermäßigungsberechtigungen, bestehende Monatskarten und Fahrerlaubnisse in einer digitalen Wallet (deutsch: Brieftasche) speichern. Dort entsteht eine sogenannte selbstbestimmte Identität (Self-Sovereign Identity, kurz: SSI), über deren Verwaltung und Weitergabe die Person dahinter selbst entscheidet. Und im Gegensatz zu klassischen Ausweisen können datensparsam nur die relevanten Informationen übermittelt werden. Anstatt wie bisher beispielsweise einen kompletten Führerschein samt Foto, Geburtsdatum und allen erlaubten Fahrzeugklassen vorzulegen, lässt sich mit einer digitalen Identifizierung lediglich der Aspekt »Fahrerlaubnis für das gewünschte Auto« nachweisen – alle anderen Führerscheindaten bleiben dem Mobilitätsdienstleister verborgen.

ID-Ideal ist Teil einer größeren Initiative, mit der die Bundesregierung seit einiger Zeit digitale Identitäten voranbringen möchte. Im September 2021 trat das Smart-eID-Gesetz in Kraft. Es legt die Grundlage dafür, dass der elektronische Personalausweis in einer Smartphone-Wallet gespeichert





»Wir wollen erreichen, dass sich in Dresden und Leipzig mit einem digitalen Fahrausweis alle Verkehrsmittel nutzen lassen, von Bussen und Bahnen bis hin zu Leihrädern, E-Scootern und Car-Sharing«, sagt Jürgen Anke, Professor für Softwaretechnologie und Informationssysteme an der HTW Dresden (oben rechts).

werden kann, sicher und binnen drei Minuten. Die Smart-eID soll 2022 für immer mehr Smartphones verfügbar werden, die die strengen Sicherheitsanforderungen erfüllen; für den geplanten Startschuss im Winter war nur ein Endgerät mit speziellem Chip vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifiziert. »Das Smart-eID-Gesetz ist ein Quantensprung für Geschäftsmodelle im Internet und digitale Kommunikation mit der Verwaltung«, sagte der für die Einführung zuständige Bundes-CIO und Staatssekretär Markus Richter mit Blick auf die Erleichterungen, die die neue Technologie bringen soll. Zwar existiert bereits seit 2010 eine Online-Ausweisfunktion, doch ist sie bisher den meisten Menschen zu umständlich: Nur sechs Prozent der Deutschen nutzen das Verfahren, für das neben dem Ausweis eine PIN, eine Software auf dem Computer und ein Lesegerät oder NFC-fähiges Smartphone nötig sind.

» Zur Identität gehören viel mehr Merkmale, als im Personalausweis stehen «

Jürgen Anke, Professor für Softwaretechnologie und Informationssysteme an der HTW Dresden

Im Gegensatz dazu soll die Smart-eID die Identifizierung gegenüber Behörden und Unternehmen einfacher machen; und die Anwendungsfälle zur Nutzung digitaler Identitäten sollen massiv anwachsen. Der Online-Personalausweis im Smartphone ist eng verbunden mit dem vom Bundeswirtschaftsministerium initiierten Innovationswettbewerb Schaufenster Sichere Digitale Identitäten. »Kommunen und Wirtschaftsunternehmen werden dabei unterstützt, digitale Identitäten in ihre Services zu integrieren«, erklärt Fabienne Eigner, die für den Wettbewerb verantwortliche Wissenschaftliche Referentin. »Im Mittelpunkt stehen aber die Bürgerinnen

und Bürger, die in den Modellregionen sichere digitale Identitäten made in Germany erleben können.« ID-Ideal in Sachsen ist eines von vier ausgewählten Projekten; weitere laufen bis 2024 in Köln/Berlin (IDunion), Hessen/Bayern/Nordrhein-Westfalen (ONCE) sowie in Karlsruhe und der Metropolregion Rhein-Neckar (SDIKA).

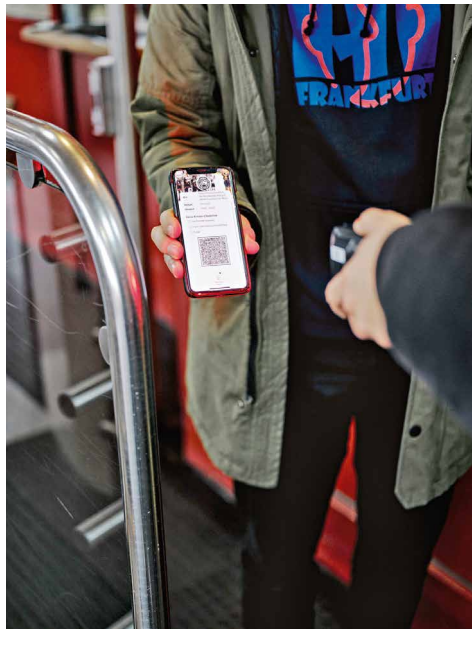
»Insgesamt erproben wir 108 Anwendungsfälle«, erklärt Martin Schallbruch, Direktor des Digital Society Institute an der ESMT Berlin, der die Begleitforschung zum Innovationswettbewerb leitet. Digitale Identitäten beziehen sich dabei nicht zwangsläufig auf Menschen; sie können auch als rechtssichere Nachweise für Unternehmen oder Dinge – beispielsweise Verleih-Geräte – dienen. »Diese Identitäten sind der Schlüssel für alle digitalen Prozesse«, betont Schallbruch und zitiert eine Civey-Studie aus dem Jahr 2021, nach der ein Viertel der Deutschen 20 bis 100 digitale Identitäten nutzen – meist verteilt auf viele verschiedene Dienstleister und oft ineffizient und unsicher verwaltet: Nur jeweils 20 Prozent der Befragten verwenden einen Passwortmanager oder speichern ihre Passwörter im Browser.

Schaufenster Sichere Digitale Identitäten arbeitet daran, ein eID-Ökosystem zu schaffen, in dem einmal erfasste Identitätsnachweise für Anwendungsfälle aller Art nutzbar sind. »Eine wichtige Herausforderung ist es, diese Interoperabilität auch über Deutschland hinaus zu gewährleisten«, sagt Schallbruch und verweist auf Bestrebungen der EU-Kommission, eine einheitliche europäische digitale Identität einzuführen. Ebenso wichtig sind Datenschutz und Sicherheit, damit digitale Identitäten überhaupt das nötige Vertrauen genießen. »Die Echtheit eines Identitätsnachweises wird mit digitalen Signaturen der ausstellenden Instanz bestätigt«, erklärt dazu Professor Anke von der HTW Dresden. »Sie werden außerdem in einem geschützten Bereich auf dem jeweiligen Smartphone gespeichert und verschlüsselt zwischen der Wallet des Nutzers und den Systemen der Dienstleister übertragen.«

Dokumente aus Papier und Plastik können ersetzt werden

Auf dezentrale Speicherung digitaler Identitäten setzen auch die Entwicklerinnen und Entwickler von Helix ID aus Frankfurt. »Unsere Smart-Wallet-App bündelt persönliche Informationen sicher und dezentral, macht umständliches Anmelden auf verschiedenen Seiten überflüssig und sorgt gleichzeitig dafür, dass die Nutzerinnen und Nutzer die Hoheit über ihre Daten behalten«, erklärt Gründer Oliver Naegele. Wer relevante Nachweise verifiziert und hinterlegt hat, kann sich damit bei verschiedenen Partnern identifizieren, mit denen das Start-up zusammenarbeitet. Zudem ist Helix ID Initiator einer Frankfurter Smart-City-Initiative, die es Einheimischen und Gästen ermöglichen soll, mit einer einzigen App etliche digitale Angebote und Dienstleistungen in der Stadt zu nutzen.

Ob in Unternehmen, Politik oder Wissenschaft: Die Zuversicht, dass digitale Identitäten Dokumente aus Papier und Plastik nach und nach ersetzen, scheint groß. »Ich denke, dass digitale Identitäten in drei bis fünf Jahren Teil unseres Alltags sind«, sagt Professor Anke. Der entscheidende Erfolgsfaktor für ihn ist die regelmäßige Anwendung für unterschiedlichste Zwecke: »Eine Identität, die ich nur ein- bis zweimal im Jahr für Behördengänge brauche, wird sich nicht durchsetzen.« •



Oliver Naegele (oben) und sein Team wollen mit ihrer Helix ID allerlei Nachweise ins Smartphone packen. So sollen Einheimische und Gäste sich mit einer App für etliche Angebote in Frankfurt identifizieren können.

Allianzen für sichere Smartphone-Identitäten

Heutige und vor allem künftige Smartphones übernehmen immer mehr Aufgaben, die eng mit der Identität ihrer Besitzer:innen zusammenhängen: Kreditkartenzahlungen vornehmen, Autos aufschließen oder sich identifizieren. Um die dahinterliegenden Daten optimal zu schützen, hat Google bereits 2018 mit dem Smartphone Pixel 3 den speziellen Sicherheitschip Titan M eingeführt und ist aktiv an der Standardisierung und Implementierung von datensparsamen mobilen Führerscheinen nach dem internationalen Standard ISO 18013-5 beteiligt.

Im März 2021 startete Google gemeinsam mit verschiedenen Partnern, darunter dem Münchner Bezahl- und Identitätsspezialisten Giesecke+Devrient, die Android Ready SE Alliance. SE steht dabei für Secure Element (»sicheres Element«). Die Allianz soll Open-Source-Programme entwickeln, die direkt auf dem separaten Sicherheitschip ausgeführt werden. So können beispielsweise digitale Identitäten höchster Sicherheitsklassen ermöglicht werden, etwa die nächste Generation der Führerscheine. »Mit diesen frei verfügbaren sogenannten Secure Applets können Gerätehersteller digitale Identitäten einfach und mit zertifizierter Sicherheit umsetzen«, sagt René Mayrhofer vom Team der Android Platform Security.

Was ist eigentlich …

Digitale Souveränität?

TEXT: CHRISTOPH HENN
ILLUSTRATION: ARI LILOAN

Viele kennen den Begriff nicht, dabei betrifft er so gut wie alle: Was es bedeutet, im digitalen Raum selbstbestimmt zu handeln und zu entscheiden

Kontrolle behalten

Souveränität entsteht, wenn wir selbst bestimmen, was von uns online bleibt

Souveräne Staaten sind unabhängig, souveräne Menschen treffen ihre eigenen Entscheidungen. Und auch digitale Souveränität hat viel mit Freiheit zu tun: Der Begriff beschreibt die Fähigkeit, im digitalen Raum selbstbestimmt zu handeln und zu entscheiden. Das gilt für einzelne Bürgerinnen und Bürger, aber auch für Unternehmen und Staaten. Der einzelne Mensch möchte sich beispielsweise frei in der digitalen Welt bewegen und selbst kontrollieren können, was mit den Informationen geschieht, die er dort hinterlässt. Firmen brauchen geeignete IT-Infrastrukturen, etwa schnelle Internetverbindungen oder ausreichende Rechen- und Speicherkapazitäten, um die digitale Transformation nach ihren Vorstellungen zu gestalten. Und Staaten wollen jederzeit Zugang zu digitalen Technologien und Daten haben, ohne dabei von anderen Staaten abhängig zu sein.

Grundlagen verstehen

Souveränität entsteht, indem wir mehr über digitale Medien erfahren

Ob beim Autofahren, in der Gartenpflege oder im Beruf: Wissen, Erfahrung und grundlegende Fähigkeiten entscheiden darüber, wie souverän jemand in einem bestimmten Themengebiet handeln kann. Deshalb ist digitale Kompetenz eine Grundvoraussetzung für digitale Souveränität. Laut dem Bundesministerium für Familie, Senioren, Frauen und Jugend geht es nicht nur darum, Smartphones, Computer und andere technische Geräte bedienen zu können – sondern um »deutlich weitergehende Fertigkeiten, die Bürgerinnen und Bürgern einen kenntnisreichen, kritischen, kreativen und widerstandsfähigen Umgang mit digitalen Medien ermöglichen«.

Sicherheit spüren

Souveränität entsteht, wenn wir digitalen Diensten vertrauen können

Nur wer vertrauen kann, wird souverän. Das spüren wir beispielsweise im Berufsleben: Eine Präsentation wirkt souverän, wenn wir in der Sache sicher sind, weil wir auf unser Wissen vertrauen. Auch im digitalen Raum ist Souveränität nicht ohne Vertrauen und Sicherheit denkbar: Wir könnten dort nicht wirklich selbstbestimmt handeln, wenn wir kein Vertrauen hätten, dass unsere Daten nicht missbraucht werden und der Datenschutz mit unseren Werten übereinstimmt. Das kritische Bewusstsein dafür ist in Deutschland mehr und mehr vorhanden. Laut einer Sonderstudie des D21-Digital-Index 2020/2021 gehen 83 Prozent der Befragten davon aus, dass manche Dienste und Apps persönliche Daten weitergeben. 74 Prozent der Menschen wiederum fühlen sich dazu in der Lage, die Datenschutzeinstellungen ihrer Apps zu verwalten.

Einstellungen prüfen

Souveränität entsteht, wenn wir selbst aktiv werden

Wichtige Voraussetzungen zum Schutz und zur Kontrolle der eigenen digitalen Identität – und damit der Souveränität – sind sichere Passwörter und weitreichende Einstellungsmöglichkeiten rund um den Datenschutz. Das Google Safety Engineering Center in München zum Beispiel arbeitet an vielen solcher Werkzeuge, die Menschen weltweit schützen, damit sie selbstbestimmt im Internet unterwegs sein können: Dazu gehören der Google Passwortmanager, der in Chrome, Android und die Google App integriert ist, der Sicherheitscheck sowie die Informationen und Einstellungsmöglichkeiten im Google-Konto. Dort können Nutzerinnen und Nutzer unter anderem festlegen, welche Aktivitätsdaten zur Personalisierung von Diensten gespeichert werden, ob Werbung personalisiert angezeigt werden soll und welche Informationen sie mit anderen teilen.

Länderübergreifend kooperieren

Souveränität entsteht durch Zusammenarbeit

Neben der digitalen Souveränität des einzelnen Menschen wurde zuletzt vor allem die politische Ebene des Begriffs diskutiert: Deutschland und die EU streben mehr digitale Unabhängigkeit an und wollen gemeinsam mit Wirtschaft und Forschung kooperieren, damit im Rahmen des »Projekts Gaia-X« eine »vertrauenswürdige Dateninfrastruktur für Europa« entsteht. Laut Bundeswirtschaftsministerium soll ein innovationsförderndes, offenes und transparentes digitales Ökosystem entstehen, in dem Daten und Dienste verfügbar gemacht, zusammengeführt, vertrauensvoll geteilt und genutzt werden können.

Flexibel bleiben

Souveränität entsteht durch eine variable Infrastruktur

Unternehmen und andere Organisationen verarbeiten, analysieren und speichern jeden Tag große Datenmengen. Um reibungsfreie Prozesse sicherstellen zu können, spielt sich heute ein Großteil der digitalen Aktivitäten über das sogenannte Cloud Computing ab. Dabei werden Speicherplatz, Rechenleistung oder Programme über das Internet bereitgestellt. Die jeweiligen Nutzer:innen profitieren von hoher Flexibilität und können je nach Bedarf jederzeit mehr oder weniger Computer-Ressourcen in Anspruch nehmen. Um auch hier maximale Souveränität zu bieten, arbeiten T-Systems und Google Cloud an einer modernen und innovativen souveränen Cloud aus Deutschland für Deutschland. Dabei werden Unternehmen, Behörden oder Gesundheitseinrichtungen jederzeit volle Kontrolle über ihre Daten haben. Google investiert in den nächsten Jahren rund eine Milliarde Euro in neue Cloud-Infrastrukturen in Deutschland – und in deren Versorgung mit sauberer Energie.

Das gezielte Rauschen

Fortschrittliche Anonymisierungsverfahren schaffen neue Möglichkeiten für Forschende: Mit Differential Privacy lassen sich personenbezogene Daten so auswerten, dass die Allgemeinheit davon profitiert – ohne einzelne Menschen zurückverfolgen zu können

TEXT: BIRK GRÜLING; ILLUSTRATIONEN: ARI LILOAN; FOTOS: IAN PATTERSON, FLORIAN GENEROTZKY

Wie viel bewegen Sie sich? Wie schwer und groß sind Sie? Rauchen Sie? Haben Sie chronische Erkrankungen? Solche Informationen über die eigene Gesundheit sind Klassiker auf jedem Ärztefragebogen und gehören doch zu den sensibelsten Daten überhaupt, vergleichbar höchstens mit dem Finanzstatus. Entsprechend hoch sind die Ansprüche und Vorgaben in Sachen Datenschutz. Ein Beispiel: Wenn ein forschendes Krankenhaus Daten zu Diabetes-Erkrankungen oder zum Lungenkrebsrisiko von Rauchern erhebt, muss die Privatsphäre der Studienteilnehmenden so gesichert sein, dass es nicht möglich ist, die Person hinter den Informationen auszumachen. Ohne ausreichende Anonymisierung dürfen die Daten nicht einmal an andere Forschungsgruppen im eigenen Haus weitergegeben werden, von einem wissenschaftlich fruchtbaren Austausch über Ländergrenzen hinweg ganz zu schweigen.

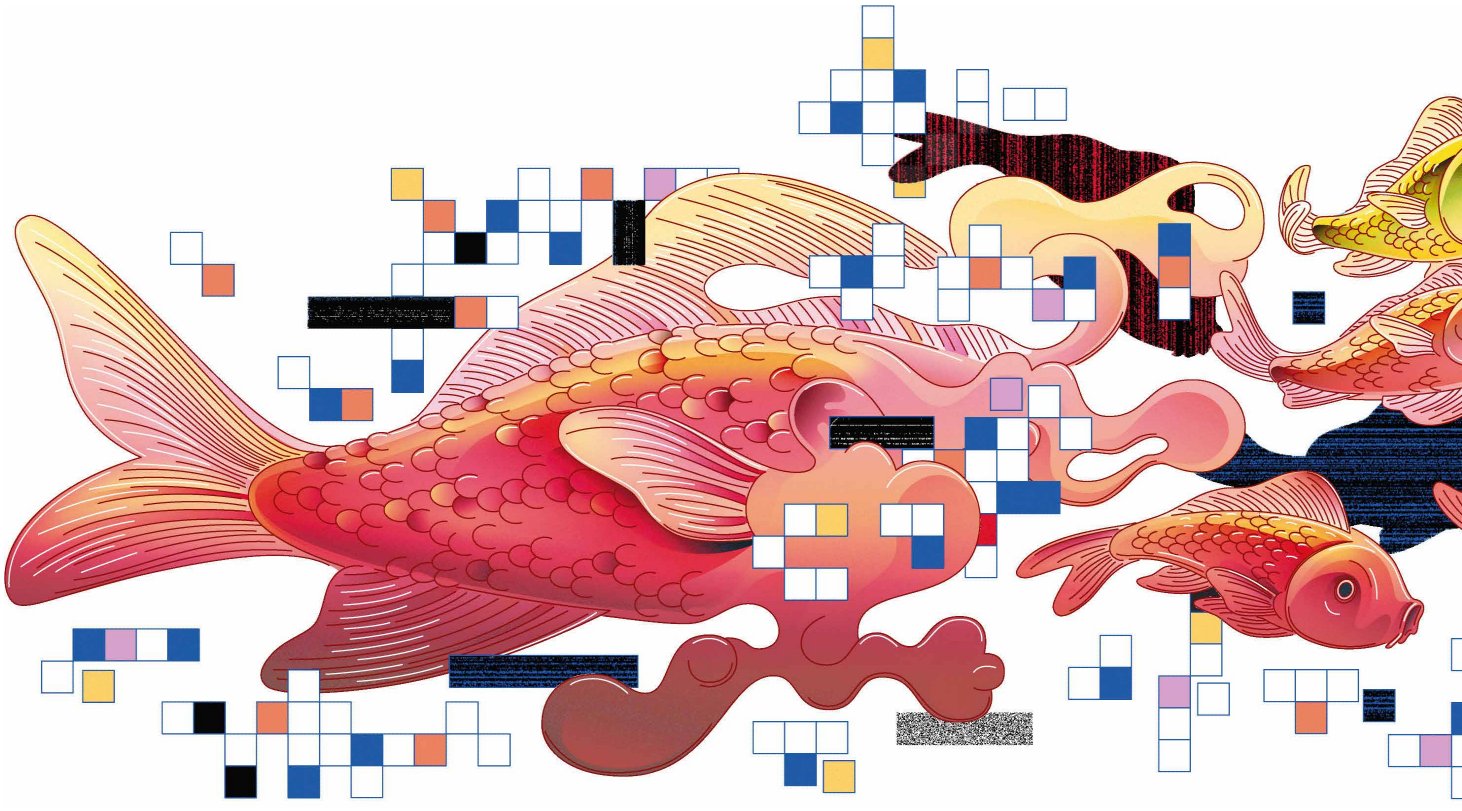
Doch warum werden nicht einfach persönlich identifizierbare Daten wie Wohnort, Name oder Geschlecht geändert oder weggelassen? »Eine solche Anonymisierung von Daten reicht in vielen Fällen nicht aus«, sagt Franziska Boenisch, IT-Security-Expertin am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC). »Gerade wenn zusätzliche Daten aus anderen, eigentlich unabhängigen Quellen dazukommen, sind Rückschlüsse auf Einzelpersonen schnell möglich. Schon Social Media Posts oder Berichte aus Tageszeitungen reichen aus.«

Was sie meint, zeigt das Beispiel eines großen Videostreaming-Anbieters. Um den Empfehlungsalgorithmus für Serien und Filme zu verbessern, lobte er einen Wettbewerb aus und stellte den IT-Fachleuten 500 000 Datensätze echter Kundinnen und Kunden zur Verfügung, ohne persönliche Daten wie Name oder Adresse. Forschende der Universität Texas konnten trotzdem eine große Zahl der Daten tatsächlichen Personen zuordnen, und zwar nur durch den Vergleich mit öffentlichen Profilen bei einer bekannten Filmbewertungsplattform. Bei Sehgewohnheiten ist ein derartiger sogenannter Verknüpfungsangriff schon sehr unerfreulich; bei anderen persönlichen Informationen wäre er noch gefährlicher: Eine Rückverfolgung von medizinischen Daten zu realen Personen wäre nicht viel komplizierter, die Folgen umso gravierender. Anonymisierte Krankenhausberichte könnten sich durch Medienberichte über seltene Krankheiten, Spendenaktionen für kranke Menschen oder Unfälle schnell echten Patientinnen und Patienten zuordnen lassen.

Mathematisches Rauschen verhindert die Rückverfolgung

Wenn also eine naive Anonymisierung nicht ausreicht, müssen neue Methoden her. Ein Verfahren, das immer mehr Unternehmen und Organisationen nutzen, ist Differential Privacy. Dieses Anonymisierungskonzept eignet sich vorrangig für Statistiken über große Datenmengen. Sehr einfach ausgedrückt geht es darum, die Abfrage der Datensätze mit einem gezielten Rauschen zufällig zu verändern, um den Beitrag eines einzelnen Individuums zur Statistik unkenntlich zu machen. Zum Beispiel wird zu

Franziska Boenisch, IT-Expertin am Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (AISEC), verbrachte bis vor Kurzem einen Forschungsaufenthalt am Vector Institute für künstliche Intelligenz in Toronto, wo auch diese Bilder entstanden. Einfache Anonymisierungen reichen Boenisch zufolge oft nicht aus, um persönliche Daten zu schützen.



jedem Datenpunkt ein zufälliger Wert addiert. »Trotz des Rauschens können aus den Datensätzen weiterhin nützliche Erkenntnisse über die Gesamtheit gewonnen und sogar veröffentlicht werden. Es lassen sich daraus viel schwerer persönliche Informationen über einzelne Personen ableiten«, erklärt Boenisch. Das Konzept der Differential Privacy sehe sogar vor, dass das Fehlen oder Vorhandensein der Daten einer einzelnen Person keinen Einfluss auf das Ergebnis der durchgeführten statistischen Auswertung haben darf.

Einen großen Vorteil der Methode erklärt Gonzalo Munilla Garrido, der Softwareentwickler beschäftigt sich an der Technischen Universität in München mit Technologien zur Verbesserung der Privatsphäre: »Mehrere Parameter legen fest, wie streng der Schutz der Privatsphäre ist.« Ein Beispiel dafür ist der Wert Epsilon, mit ihm lässt sich das Rauschen über den Daten dosieren – je nach Anwendung. Ein kleiner Wert schützt zwar die Privatsphäre sehr gut, macht die Datenanalyse aber schwieriger. Ein großer Wert gibt dagegen mehr Informationen preis.

Auch Google nutzt Differential Privacy in verschiedenen Anwendungen. Ein simples Beispiel ist die Angabe über den durchschnittlichen Besucherandrang in öffentlichen Einrichtungen in Google Maps und der Google Suche. Das hilft Menschen, gerade in Zeiten einer Pandemie, Stoßzeiten beim Einkaufen oder im Museum zu meiden. Ob für diese Funktion jedoch 999 Personen als Datengrundlage dienen oder 1000 ist nicht relevant, und auch über die Personen, die gerade vor Ort sind, braucht es keine Informationen. »Die Identität jeder einzelnen Person im Datensatz ist bei einer Analyse dank des differenzierten Datenschutzes gleichermaßen geschützt, selbst wenn es andere zusätzliche Informationsquellen gibt, die Angreifer gemeinsam nutzen könnten, um die Identität der Personen aufzudecken«, sagt Garrido. Auch für die sogenannten Mobilitätsberichte, die Google im Kampf gegen die Corona-Pandemie öffentlich bereitstellt, wird Differential Privacy genutzt.

Neben Tech-Konzernen wie Google, Apple oder SAP schützt beispielsweise auch die US-Regierung die Daten aus ihrer aktuellen Volkszählung damit. So sollen sie zwar Erkenntnisse über Alters- oder Sozialstrukturen zulassen, aber nicht über bestimmte Individuen innerhalb einer Gesellschaft. Auch in Deutschland laufen zahlreiche Differential-Privacy-Testläufe. Beim Projekt »WerteRadar« etwa kooperieren unter anderem die Berliner Charité, das Fraunhofer AISEC, die Freie Universität Berlin und die Fernuni Hagen. Ziel ist es, eine interaktive Software zu entwickeln, die Patient:innen dabei hilft, über die Weitergabe ihrer Gesundheitsdaten souveräner zu entscheiden. Zur Anonymisierung von Gesundheitsdaten wird dabei auch Differential Privacy genutzt.

Open-Source-Bibliothek für Start-ups und Forschende

Google arbeitet nicht nur für eigene Zwecke an und mit Differential Privacy. Am Google Safety Engineering Center (GSEC) in München sorgen Entwickler:innen dafür, dass die Bausteine dafür öffentlich und kostenlos zugänglich sind. Um allen Forschenden, Organisationen, Unternehmen und Start-ups die technisch mitunter komplexe Nutzung von Differential Privacy zur Auswertung und Sicherung ihrer Daten zu ermöglichen, hat Google 2019 die entsprechende Open-Source-Bibliothek veröffentlicht. »Kaum ein Geschäftsmodell kommt heute ohne die Erhebung und Analyse von Daten aus. Gerade Start-ups wollen wir deshalb durch freie Algorithmen dabei unterstützen, Daten verantwortungsbewusst zu nutzen und personenbezogene Informationen zu schützen«, erklärt Christoph Dibak, der im GSEC an der Differential-Privacy-Bibliothek arbeitet. Auch an Forschende richtet sich das Angebot. Sie können mit den freien Werkzeugen ihre Studiendaten so absichern, dass sie später veröffentlicht werden können, ohne den Datenschutz zu verletzen.

Das GSEC stellt nicht nur Algorithmen zur Verfügung, sondern veranstaltet auch öffentliche Schulungen, sogenannte Codelabs, zu Differential Privacy sowie Community Events, bei denen Entwicklerinnen und Entwickler und andere Interessierte Fachfragen austauschen können. Zudem bietet das GSEC weitere freie Tools an, zum Beispiel zur Testung der Differential-Privacy-Algorithmen. Auch Softwarelösungen für Entwickler:innen ohne tiefere Kenntnisse von Differential Privacy sind frei verfügbar. Wenn solche Lösungen ohne entsprechendes Know-how selbst programmiert werden, komme es dagegen oft zu Fehlern und damit zu Risiken für persönliche Daten, sagt Softwareentwickler Dibak.

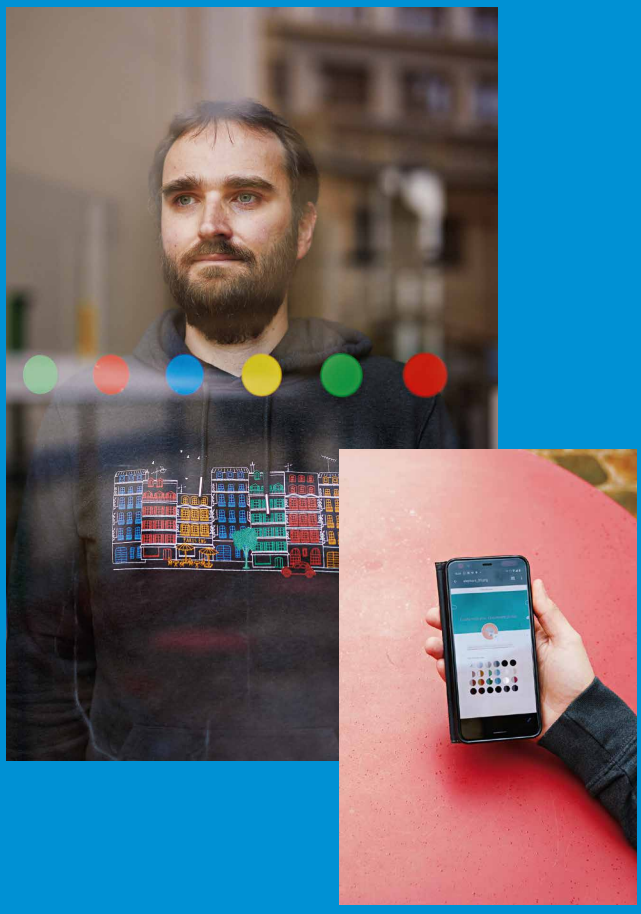
Natürlich ist auch Differential Privacy im Datenschutzkosmos nur ein Baustein von vielen. »Die Methode kann dabei helfen, Datensätze sehr gut zu anonymisieren und persönliche Daten zu schützen«, erklärt Boenisch. »Aber es braucht auch Schutz vor der Anonymisierung, zum Beispiel bei der Erhebung und Verarbeitung der Daten.« Auch zu diesem Problem gibt es bereits Lösungsansätze, an denen unter anderem Google-Teams arbeiten. •

Der Softwareentwickler Gonzalo Munilla Garrido beschäftigt sich an der TU München mit Anwendungsszenarien von Differential Privacy.

Sie stärken die Privatsphäre im Internet

PROTOKOLLE: KATHARINA FUHRIN/CHRISTOPH HENN
FOTOS: SIMON HABEGGER, STEPHANIE FÜSSENICH
SIMA DEHGANI (7), MARIA HAEFNER (1)

Im Münchner Google Safety Engineering Center (GSEC) arbeiten mehrere Hundert Spezialist:innen an innovativen Lösungen für ein sicheres Internet. Hier berichten sieben von ihnen, wie Nutzer:innen auf der ganzen Welt von dieser Arbeit profitieren



Chrome-Profile: Privatsphäre für gemeinsame Computer

Softwareentwickler David Roger und seine Kolleg:innen haben die Profile in Chrome runderneuert. Damit können mehrere Menschen noch bequemer auf demselben Gerät im Internet surfen.

»Wenn mehrere Personen denselben Computer benutzen, surft meist auch jede mit demselben Browser. Das aber hat zur Folge, dass mir zum Beispiel auf YouTube Inhalte angezeigt werden, die für mich gar nicht interessant sind. Dass ein falsches Passwort eintragen wird, wenn ich mich auf einer Website einloggen möchte. Oder dass andere meine E-Mails sehen. Das ist natürlich ein großes Problem für die digitale Privatsphäre. Eine ähnliche Situation liegt vor, wenn ich einen Computer sowohl privat als auch für die Arbeit nutze – dann muss ich sogar aufpassen, dass ich dabei nicht meine privaten mit meinen geschäftlichen Daten vermische. Lösen können wir diese Herausforderung mit den Profilen in Chrome. Wir haben sie runderneuert, sodass sie nun viel einfacher zu finden und zu benutzen sind. Nutzer:innen können jetzt schnell und einfach ein oder mehrere eigene Profile anlegen und sie mit der Lieblingsfarbe versehen. So wird Chrome zu einem persönlichen Browser, der die individuelle Privatsphäre auch auf gemeinsam genutzten Geräten schützt.«

Datenschutzchecks: Schwachstellen aufdecken und beheben

Rebecca Balebako und ihr Team prüfen, ob Privatsphäre-funktionen richtig arbeiten und wie sie sich weiter verbessern lassen. Und sie beraten Google-Kolleg:innen und Start-ups in Datenschutzfragen.

»Unser Team bildet eine von mehreren Datenschutzebenen bei Google: Wir tun manchmal so, als wären wir selbst die Angreifer, und suchen unser eigenes System nach Schwachstellen ab. Wenn es eine gibt, dann wollen wir das so schnell wie möglich wissen und sie beheben. Dabei nehmen wir uns in jedem Quartal ein anderes Google-Produkt vor und testen es auf Herz und Nieren darauf, ob es die Privatsphäre unserer Nutzer:innen wie versprochen gewährleistet. Auch wenn in der Regel alles so funktioniert wie geplant: Datenschutz lässt sich immer weiter optimieren. Dabei ist es meine Aufgabe, die richtigen Fragen zu stellen: Was wollen die Nutzerinnen und Nutzer? Was brauchen sie? Und wie können wir diese Fragen beantworten? Zu unserer Arbeit gehört es auch, andere zu unterstützen. Deshalb wenden wir im GSEC diese Herangehensweise auch an, wenn wir Start-ups in einem sehr frühen Stadium zum Thema Datenschutz beraten. Es ist spannend, andere Unternehmen kennenzulernen und zu verstehen, was deren Probleme sind. Denn selbst wenn jemand zum Beispiel mit Stahl handelt – an irgendeiner Stelle geht es immer um Datenschutz.«

Privatsphäre-Tools:
Optionen für viele Bedürfnisse

Die Softwareentwicklerin Kader Belli kümmert sich darum, dass Nutzer:innen auf unterschiedliche Weise Einstellungen für ihre Privatsphäre vornehmen können – aber immer möglichst simpel.

»Ich bin für einige Bereiche im Google-Konto zuständig, die Transparenz und Einstellungsmöglichkeiten rund um das Thema digitale Privatsphäre bieten sollen. Dazu gehören hauptsächlich diese vier: Erstens der Privatsphärecheck, mit dem sich wichtige Datenschutzeinstellungen prüfen und anpassen lassen. Zweitens das Google Dashboard, das einen Überblick über alle verwendeten Google-Dienste und die dort gespeicherten Aktivitätsdaten gibt. Drittens der Google Datenexport, wo Nutzer:innen gezielt persönliche Kontodaten herunterladen und bei Bedarf zu einem anderen Anbieter exportieren können – wie zum Beispiel Fotos. Und viertens die ›Meine Daten‹-Abschnitte, die erklären, wie die Dienste Google Maps, Google Suche, YouTube und Google Assistant bestimmte Daten zur Personalisierung nutzen. Bei all diesen Bereichen legen wir großen Wert darauf, dass sie sowohl nützlich als auch verständlich und leicht auffindbar sind. Wir befragen dafür regelmäßig unsere Nutzer:innen, um ihre Bedürfnisse zu verstehen. Der Schutz und die Regulierung der eigenen Privatsphäre im Internet sollten so simpel wie möglich sein.«

Browser-Einstellungen:
Personalisieren und sichern

Martin Šrámek ist als Manager für die Datenschutzeinstellungen in Chrome zuständig. Sie erlauben es Nutzer:innen, ein individuelles Maß an Surfkomfort und Privatsphäre zu justieren.

»Viele denken, dass die Privatsphäre beim Surfen im Internet nur dann geschützt ist, wenn der Browser überhaupt keine Daten speichert oder sendet. Daten können aber genutzt werden, ohne die Privatsphäre zu verletzen, und ihre Verwendung bringt den Nutzer:innen viele Vorteile: Chrome kann dadurch personalisiert und das Surferlebnis verbessert werden. Dafür geben wir Nutzer:innen Einstellungsmöglichkeiten. Sie können auswählen, inwieweit sie von den Personalisierungen profitieren möchten. Hier lässt sich auch einsehen, welche Aktivitätsdaten Chrome speichert, etwa den Verlauf der besuchten Internetseiten oder Cookies; und sie lassen sich an Ort und Stelle löschen. Wir verstehen aber auch, dass sich viele nicht tiefergehend mit diesem Thema beschäftigen möchten, um aktiv Datenschutzentscheidungen zu treffen. Daher gibt es Voreinstellungen, die für die meisten Nutzer:innen einen guten Kompromiss zwischen Privatsphäre und Surfkomfort darstellen sollen. Unsere Devise dabei ist: Du hast Einstellungsmöglichkeiten, um deine Privatsphäre nach deinen Wünschen zu gestalten. Und wenn du nichts machst, gelten die Voreinstellungen.«

Google-Konto:
Alles an einem Platz

Werner Unterhofer trägt als Technical Program Manager dazu bei, dass sich wichtige Datenschutzeinstellungen von einem Ort aus bearbeiten lassen.

»In München entwickeln und bauen wir das Google-Konto, das auf der ganzen Welt genutzt wird. Das Kernstück ist die Seite ›Daten und Datenschutz‹, auf der sich wichtige Einstellungsmöglichkeiten zu Datenschutz, Personalisierung und dem Teilen von Daten befinden, die wir basierend auf Nutzerfeedback kontinuierlich weiterentwickeln. Dort zeigen wir den Nutzer:innen die verschiedenen Optionen, wie Google-Dienste für sie relevanter werden, wenn sie sich dafür entscheiden, bestimmte Informationen mit Google zu teilen – Suchgewohnheiten etwa oder Standortverläufe. Im Google-Konto lässt sich auch einsehen, welche Aktivitätsdaten gespeichert sind, und diese lassen sich dort herunterladen oder löschen – alles gebündelt an einem Platz. Wir bemühen uns, die Privatsphäreeinstellungen so leicht zugänglich wie möglich zu machen. Deshalb lassen sie sich etwa über Suchbegriffe wie ›Datenschutzeinstellungen Google-Konto‹ in der Google Suche erreichen. Aus den meisten Google-Produkten und -Apps führt zudem ein Klick auf das Profilbild und ›Google-Konto verwalten‹ zu den Einstellungen. Datenschutz muss verständlich und leicht navigierbar sein – und nicht nur ein Thema für Fachleute.«

Privatsphäre für Familien:
Datenschutz kinderleicht machen

User-Experience-Forscherin Anja Dinhopl fokussiert sich auf die Datenschutzbedürfnisse von Kindern und Jugendlichen – und bereitet Informationen altersgerecht auf.

»Auch Kinder und Jugendliche machen sich Gedanken darüber, welche Spuren sie beim Surfen im Internet hinterlassen. Sie haben oft ganz praktische Fragen, zum Beispiel: Ist es sicher, Cookies zu akzeptieren? Was sind eigentlich Daten? Und was macht Google damit? Wir laden Kinder ein, uns ihre Fragen zu stellen, etwa in offenen Gruppendiskussionen oder über ihre Lehrerinnen und Lehrer. Denn wir möchten wissen, welche Bedürfnisse Familien mit Kindern haben, wie sie Google-Produkte nutzen und wie wir sie bei ihren Einstellungen unterstützen können. Da Kinder klare und deutliche Antworten brauchen, haben wir Datenschutzinformationen in Form eines Frage&Antwort-Formats entwickelt und sie für drei verschiedene Altersklassen aufbereitet. Das Maskottchen ist ein kleiner Pandabär. Wir haben uns sehr intensiv damit beschäftigt, welche Illustrationen passen und welche Worte die richtigen sind. Das Ergebnis gibt es inzwischen schon in 60 Sprachen.«

Datenschutzerklärung: Einfach verständlich

Von wegen komplizierte Textwüste: Kateryna Atamanchuk und ihre Kolleg:innen sorgen dafür, dass die Google-Datenschutzerklärung leicht zu verstehen ist – mit Texten, Videos und vielen nützlichen Links.

»Die Datenschutzerklärung ist eine der wichtigsten Seiten jedes Internet-Angebots, aber oft auch eine der unbeliebtesten. Das liegt daran, dass sie sehr unterschiedliche Funktionen erfüllen muss: Sie ist zum einen ein gesetzlich vorgeschriebenes Rechtsdokument, zum anderen soll sie interessierten Nutzerinnen und Nutzern verständlich erläutern, wie unsere Dienste funktionieren und wie wir mit ihren Daten umgehen. Im GSEC haben wir uns der Herausforderung gestellt, diese beiden Aspekte in Einklang zu bringen. So erklären wir viele Begriffe und Themen in kleinen, mit Beispielen versehenen Texten, die nach einem Mausklick aufploppen. Zudem ist die Seite übersichtlich strukturiert, und kurze Videos zeigen anschaulich, warum Google bestimmte Daten erhebt und wie sich individuelle Datenschutzeinstellungen vornehmen lassen. Diese Einstellungsmöglichkeiten und andere Privatsphäre-funktionen können die Nutzer:innen direkt von der Datenschutzerklärung aus aufrufen. Als Softwareentwicklerin sorge ich dafür, dass Textänderungen umgesetzt werden und die Seite jederzeit und auf allen Endgeräten stabil läuft – und zwar nicht nur auf Deutsch: Die Datenschutzerklärung existiert in 61 Sprachen, alle Versionen werden vom GSEC in München technisch betreut.«

Mitten in München: Das Google Safety Engineering Center

In der bayerischen Landeshauptstadt steht bei Google die technische Produktentwicklung im Vordergrund. Mittlerweile arbeiten mehr als 1500 Mitarbeiter:innen unter anderem auch im Google Safety Engineering Center (GSEC), einem globalen Entwicklungszentrum für Onlinesicherheit und Datenschutz, das seit 2019 am Münchner Standort angesiedelt ist. Im GSEC werden datenschutz- und sicherheitsrelevante Teile des Google Browser Chrome oder des Google-Kontos entwickelt.

Einstellungssache

Wie Sie Ihre digitale Privatsphäre in verschiedenen Google-Diensten ganz einfach managen können

Überblick

Der Datenschutzbereich im Google-Konto ist Ihre Privatsphäre-Zentrale. Hier können Sie unter anderem sehen und einstellen, welche Aktivitätsdaten in Ihrem Konto gespeichert werden, ob angezeigte Werbung personalisiert werden soll und welche Informationen Sie mit anderen teilen. Einfach ins Google-Konto einloggen und im Menü links auf »Daten und Datenschutz« klicken (oder in der Mitte auf »Daten und Datenschutz verwalten«). → *myaccount.google.com*

Privatsphäre

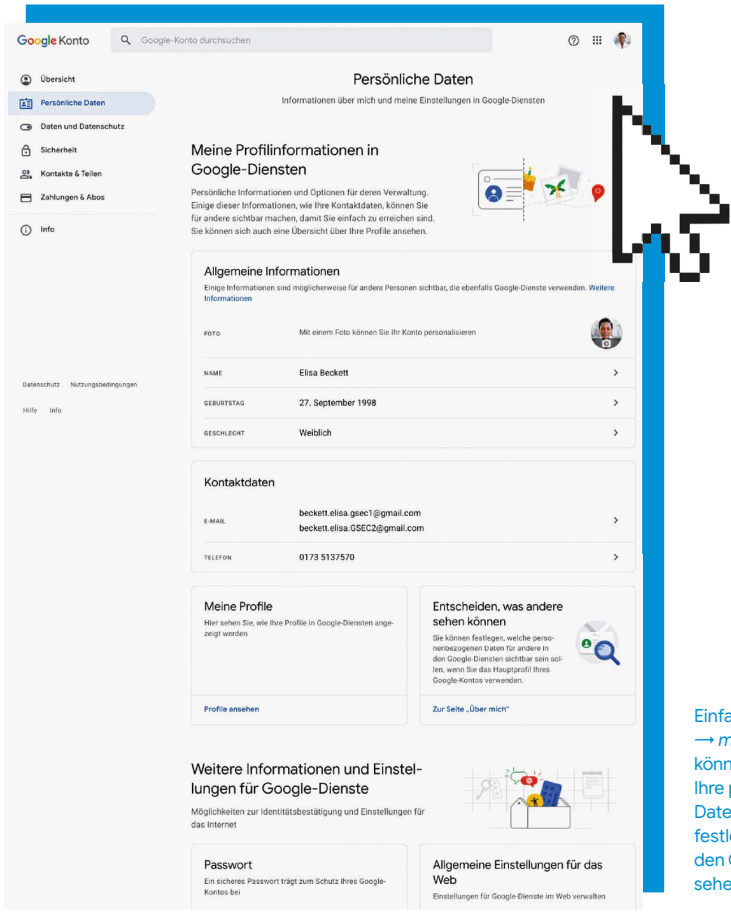
Basierend auf den Google-Diensten, die Sie am meisten verwenden, erhalten Sie mit dem Privatsphärecheck konkrete Datenschutztipps. Hier erfahren Sie beispielsweise, wie Sie Ihre Web- & App-Aktivitäten automatisch löschen oder wie Sie festlegen können, was mit Ihren Daten geschehen soll, wenn Sie Ihr Konto nicht mehr verwenden.

Aktivitätsdaten

Mithilfe der gespeicherten Aktivitäten kann Google Dienste für Sie nützlicher gestalten, etwa durch verbesserte Suchergebnisse oder relevantere Empfehlungen. Im Bereich »Meine Google-Aktivitäten« sehen Sie, welche Aktivitäten im Internet und in Apps sowie welche Standort- und YouTube-Verläufe gespeichert wurden. Sie können diese auch durchsuchen, manuell löschen oder Zeiträume einstellen, nach denen sie automatisch gelöscht werden. → *myactivity.google.com*

Seitenberechtigungen

Wer im Chrome-Browser auf das Schlosssymbol links neben der Adressleiste klickt, sieht unter anderem, welche Cookies die Seite verwendet und ob sie beispielsweise auf Mikrofon, Kamera oder Standort zugreift. Mit einem Klick auf »Website-Einstellungen« können Sie die Cookies löschen und Berechtigungen anpassen.



Einfach einstellen: Auf → *myaccount.google.com* können Sie unter anderem Ihre personenbezogenen Daten verwalten und festlegen, wer sie in den Google-Diensten sehen darf.

Passwörter

In Chrome, Android und der Google App ist der kostenlose Google Passwortmanager integriert. Er generiert starke Passwörter, speichert sie und fügt sie mit einem Klick auf Webseiten ein, wenn Sie in Ihr Google-Konto eingeloggt sind. Außerdem können Sie mit dem integrierten Passwortcheck Ihre gespeicherten Passwörter prüfen lassen, um die Sicherheit Ihrer Konten zu erhöhen. → *passwords.google.com*

Inkognitomodus

Nicht nur für das Browsen im Internet gibt es einen Inkognitomodus. Neben Chrome lässt er sich auch in den Smartphone-Apps von YouTube und Google Maps verwenden. Wenn Sie auf Ihr Profilbild und dann auf »Inkognitomodus aktivieren« tippen, werden Browserverlauf und Cookies nach der Session gelöscht bzw. Videos oder gesuchte Orte nicht in Ihrem Google-Konto gespeichert.

Chrome-Profile

Wer sich einen Computer mit anderen teilt, sollte unterschiedliche Profile im Chrome-Browser anlegen. So surfen alle für sich, und die Daten sind sauber getrennt. Einfach beim Starten von Chrome ein Profil hinzufügen und nach Belieben gestalten.

Text: Christoph Henn; Screenshot: Google

Werbung im Wandel

Damit Werbeanzeigen für Nutzer:innen relevant sind, werden sie oft auf Basis personenbezogener Daten ausgespielt. Was bedeutet das für die digitale Privatsphäre? Wie lässt sich die Datennutzung konfigurieren? Und was ändert sich in Zukunft? Wichtige Fragen und Antworten rund um Datenschutz und Werbung

TEXT: GRETA SIEBER; ILLUSTRATIONEN: ARI LILOAN

Warum gibt es Werbung im Internet?

Online-Werbeanzeigen spielen eine wichtige Rolle bei der Finanzierung von Inhalten, zum Beispiel auf Nachrichtenwebseiten, in Blogs, bei Spielen und Videos. Die Onlinewerbung ermöglicht es Werbetreibenden besser als mit analogen Anzeigen, ihre Zielgruppe zu erreichen.

Welche Anzeigenprodukte bietet Google an?

Google verfügt über ein breites Angebot an Werbeprodukten, die Unternehmen jeder Größe – vom lokalen Bäcker bis zum multinationalen Konzern – dabei helfen, ihre Zielgruppe zu erreichen und die Wirksamkeit ihres Marketings zu messen. Google zeigt Werbeanzeigen unter anderem in der Google Suche, in Form von Bannern auf Webseiten oder in Apps, und im Rahmen von YouTube, wo sie meist vor oder während eines Videos auf der Plattform zu sehen sind.

Werbung in Google-Produkten ist immer eindeutig mit dem Wort »Anzeige« gekennzeichnet. Anzeigen erscheinen zum Beispiel, weil Nutzer:innen nach bestimmten Begriffen suchen, oder weil deren Alter, Wohnort oder Interessen mit der Zielgruppe des Werbetreibenden übereinstimmen.

Google hat strenge Werberichtlinien, die verhindern, dass persönliche Informationen wie der Inhalt von E-Mails und Dokumenten, Gesundheitsdaten, ethnische Zugehörigkeit, Religion und sexuelle Orientierung für Werbung verwendet werden.

Welche Vorteile bietet personalisierte Werbung?

Von personalisierter Werbung können sowohl Nutzer:innen als auch Werbetreibende profitieren. Nutzer:innen bekommen Anzeigen und Angebote gezeigt, die möglichst interessant und passend für sie sind. Einer repräsentativen Verbraucherumfrage der Unternehmensberatung McKinsey aus dem Jahr 2019 zufolge entscheiden sich 46 Prozent der befragten deutschen Konsument:innen bewusst für personalisierte Werbung. Unternehmen, die personalisierte Anzeigen schalten, erreichen mit größerer Wahrscheinlichkeit potenzielle Kund:innen, zum Beispiel mit Babybedarf für frischgebackene Eltern.

Was sind Cookies?

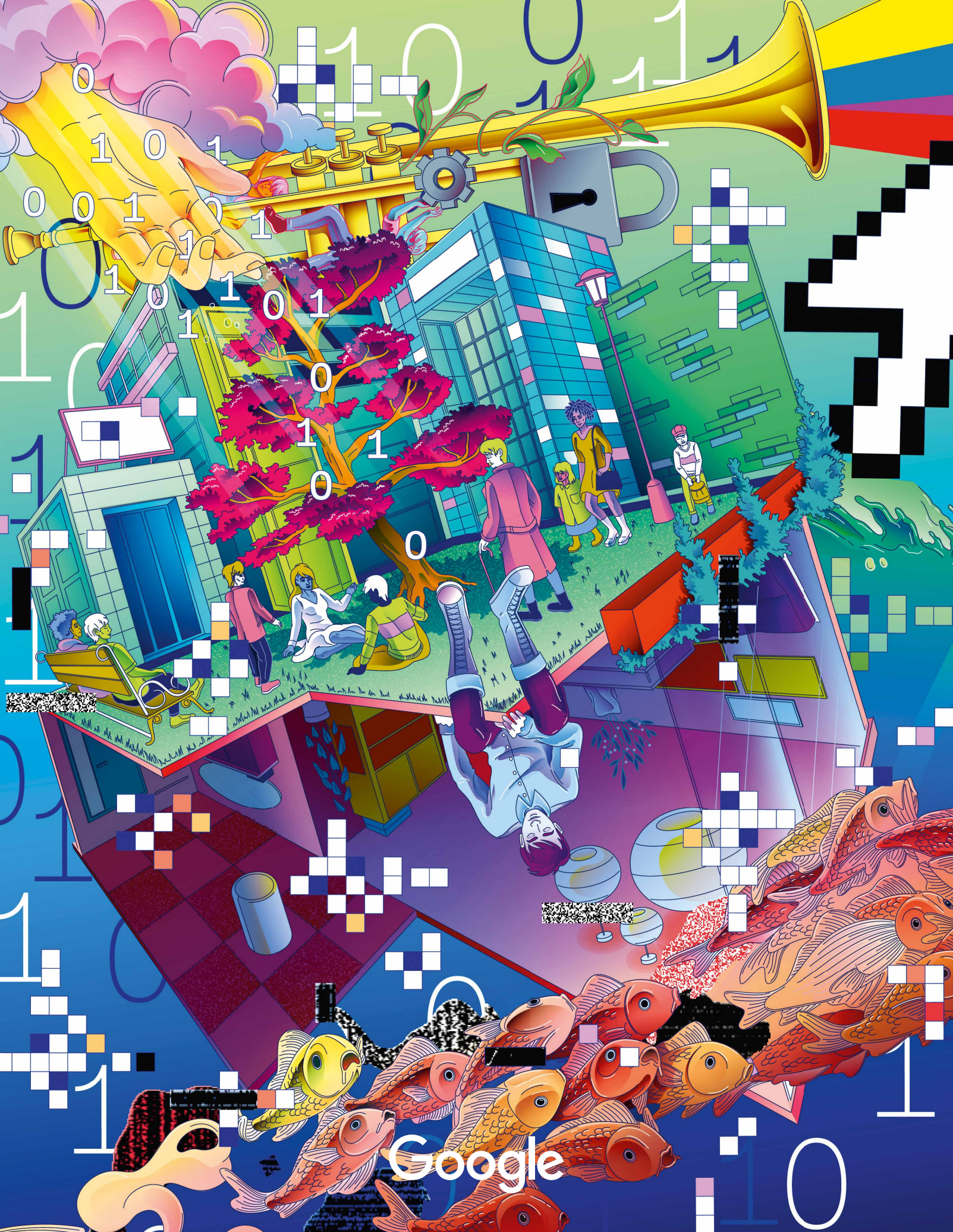
»Cookies« sind kleine Textdateien, die beim Surfen auf Webseiten erstellt und auf dem Computer gespeichert werden. Diese Dateien dienen verschiedenen Zwecken: Sie können beispielsweise dafür sorgen, dass sich Nutzer:innen auf einer Webseite nicht jedes Mal neu anmelden oder ihre Daten angeben müssen, auch die bevorzugte Sprache wird mit Cookies gespeichert. Zudem helfen Cookies Webseiten, das Surfverhalten von Nutzer:innen zu analysieren. Auf Basis dieser Informationen können Werbetreibende Nutzer:innen Werbung präsentieren, die zu ihnen und ihren Interessen passen. Dafür werden zwei Arten von Cookies eingesetzt: Eigene Cookies erstellt die Webseite, auf der jemand gerade surft. Drittanbieter-Cookies stammen von Datenhändlern oder Werbefirmen, die das Surfverhalten auf verschiedenen Webseiten speichern.

Wie können Google-Nutzer:innen die Anzeigen beeinflussen, die sie angezeigt bekommen?

Dafür gibt es mehrere Möglichkeiten: Neben jeder Werbeanzeige in den Google-Suchergebnissen findet sich ein kleines Dreieck. Wer darauf klickt, erfährt, warum diese Werbung angezeigt wird, und kann in bestimmten Fällen sogar Informationen über das werbetreibende Unternehmen abrufen. Außerdem lässt sich die Anzeige oder jegliche Werbung des Anbieters ausschalten. Über einen Link gelangen Nutzer:innen von hier aus auch in die »Einstellungen für Werbung« im Google-Konto (→*adssettings.google.com*): Dort lässt sich personalisierte Werbung konfigurieren – etwa durch die Löschung einzelner Interessen – oder generell deaktivieren.

Was ändert sich bei Online-Werbeanzeigen?

Das Ökosystem der digitalen Werbung wandelt sich – und die Cookies von Drittanbietern stehen im Mittelpunkt dieses Wandels. Viele Nutzer:innen sehen den Umgang mit Drittanbieter-Cookies und verdecktes Tracking kritisch. Sie möchten wissen, welche Daten von ihnen gesammelt werden, wie sie verwendet werden und an wen sie weitergegeben werden. Die höheren Erwartungen der Nutzer:innen an den Datenschutz haben bereits zu mehr Vorschriften und Beschränkungen für Cookies geführt. Es ist zu erwarten, dass diese Entwicklung weitergeht. Deshalb kündigte Chrome im vergangenen Jahr an, Cookies von Drittanbietern in Zukunft nicht mehr zu unterstützen. Gemeinsam mit der gesamten Branche arbeitet Google im Rahmen der Privacy Sandbox Initiative an offenen Standards, die den Datenschutz im Web grundlegend verbessern sollen. Ziel ist es unter anderem, verdecktes Tracking zu unterbinden und das Web so offen und funktional zu halten, wie es alle kennen. Mehr zu den Anstrengungen auf →*privacysandbox.com* •


Google