



DIGITALE IDENTITÄT

DER GROSSE REPORT ZUR ZENTRALEN ZUKUNFTSTECHNOLOGIE

BUSINESS Staat und Wirtschaft: Das Geschäft hinter den Daten

TECHNOLOGIE Blockchain und Silo: die technologische Seite der Identität

KONSUMENT:INNEN Wer hat die Macht über die eigenen Daten?

PHILOSOPHIE Wer bin ich und was bedeutet meine digitale Identität?

SCHRAMBÖCK · LIESSMANN · MAYER-SCHÖNBERGER · PINT · KRAMMER



WER KENNT DIESE FRAU?*

WAS IDENTITÄT UND KI MIT DIESEM BILD ZU TUN HABEN AB SEITE 3



Jetzt
**3 Monate
kostenlos
testen***

George Pro

Für kleine Unter-
nehmen und
große Projekte.

* Nach Ablauf der 3 Monate kostet George Pro 6,99 Euro/Monat.



*»Viel Vergnügen
beim Lesen unseres
ersten großen
Reports zum Thema
,Digitale Identität'!«*

OLIVER JANKO
Chefredakteur

LIEBE LESERINNEN UND LESER!

Der Begriff der „Identität“ wird nicht umsonst seit der Antike diskutiert und analysiert. Wer sind wir und was macht aus, wer wir sind? Identitäten können vielfältig sein: national, europäisch, bezogen auf Verein oder Job, auf das soziale Umfeld oder auf digitale Erscheinungsformen. Wer ich bin, bestimme ich selbst, die Legitimierung gibt aber der Staat als übergeordnete Instanz vor. Diese fehlt im Internet. Seit Jahren schwirrt auch darum der Begriff der „digitalen Identität“ durch die Medien des Kontinents - immerhin hat sich bereits vor Jahren auch die Europäische Union dieses Themas angenommen. Künftig sollen wir alle neben unserer analogen Identität, bestätigt durch Geburtsurkunde und Reisepass, auch eine eigene Identität für den digitalen Raum erhalten.

Wir haben uns auf den nächsten rund 60 Seiten angesehen, was das bedeutet - aus Sicht von Konsumentinnen und Konsumenten, aus Sicht der Wirtschaft und aus einer philosophischen Betrachtungsweise heraus. Expertinnen und Experten erklären außerdem, wie sicher der technologische Unterbau der einzelnen ID-Lösungen ist.

Während im oberösterreichischen Kremsmünster die ID Austria bereits getestet wird, haben etwa sechs Millionen Österreicher:innen noch nicht einmal die Handysignatur installiert. Dieses Ungleichgewicht soll künftig angegangen werden. Es gibt allllerdings viele Aspekte, die dabei bedacht werden müssen. Diese Magazin soll die relevantesten Thematiken beleuchten und diskutieren. Ich bedanke mich an dieser Stelle bei allen Interviewpartner:innen und den zahlreichen Expertinnen und Experten, die bei der Umsetzung des ersten Reports zum Thema „Digitale Identität“ geholfen haben. Ihnen, liebe Leserinnen und Leser, wünsche ich viel Freude bei der Lektüre! **///**

*DIE FRAU AUF UNSEREM COVER

Falls Sie sich gefragt haben, wer da vom Titelblatt lächelt: Diese Frage kann Ihnen nur unsere KI beantworten. Sowohl sämtliche Porträtbilder, die das Mosaik zusammen setzen, als auch das Foto als großes Ganzes wurden von einer Artificial Intelligence geschaffen - es gibt sie gar nicht. Warum gerade diese Person? Die Wahrscheinlichkeit, dass die AI eine junge asiatische Frau wählt, ist einfach groß. Denn der Altersmedian liegt weltweit bei 30,9 Jahren, 4,6 Milliarden Menschen weltweit stammen zudem aus Asien. Das Beispiel soll veranschaulichen, wie einfach es heute ist, authentisch wirkende Identitäten digital zu konstruieren.



06
DIGITALE
IDENTITÄT:
VIELE WEGE,
EIN ZIEL

24
»MANIPULATION
DARF NIE
UNSERE
DEMOKRATIE
GEFÄHRDEN«



34
DIE NEUE
ART DES
AUSWEISE(N)S

INHALT

DIGITALE IDENTITÄT 2021

3
Editorial
66
Impressum

12
BUSINESS
STAAT UND WIRTSCHAFT:
DAS GESCHÄFT HINTER DEN DATEN

46
KONSUMENT:INNEN
WER HAT DIE MACHT
ÜBER DIE EIGENEN DATEN?

32
TECHNOLOGIE
BLOCKCHAIN UND SILO: DIE TECHNO-
LOGISCHE SEITE DER IDENTITÄT

58
PHILOSOPHIE
WER BIN ICH UND WAS BEDEUTET
MEINE DIGITALE IDENTITÄT?



52

**BRAVE NEW WORLD
VS. 1984**



64
**»MASCHINEN
FÜHREN
(NOCH) KEIN
LEBEN«**



48

**DIGITALE
IDENTITÄT
UND DER
STAAT**

06

**DIGITALE
IDENTITÄT: VIELE
WEGE, EIN ZIEL**

Wie es um die digitale
Identität in Österreich
steht

14

**GESCHÄFTS-
MODELL DIGITALE
IDENTITÄT**

Startups und
Unternehmen aus dem
DI-Sektor im Überblick

20

**BANKEN, BOTS
& DIGITALE
BÖRSEN**

Die Rolle der Banken
für die digitale
Authentifizierung

24

**»MANIPULATION
DARF NIE UNSERE
DEMOKRATIE
GEFÄHRDEN«**

Bundesministerin
Margarete Schramböck
im Interview

26

**»SCHAFFEN EINE
IDENTITÄT FÜR
WIRTSCHAFT UND
KONSUMENT:INNEN«**

PSA-Chef Harald
Flatscher im Interview

28

**»WIR STEHEN VOR
DEM VIELFALTS-
DILEMMA«**

Christoph Mammerler,
Business Developer bei
CRIF, im Gespräch

34

**DIE NEUE ART DES
AUSWEISE(N)S**

Die Technologie hinter
den Wallets im Detail

38

**»ES MUSS EIN
POLITISCHER WILLE
ENTSTEHEN«**

Gerhard Krammer für
den Verein für digitales
Vertrauen im Gespräch

42

**KAMPF GEGEN
BETRUG**

E-Commerce-Händler:-
innen über ideale
Identifikationslösungen

48

**DIGITALE
IDENTITÄT UND
DER STAAT**

In Kremsmünster wird
die ID Austria schon
getestet

52

**BRAVE NEW
WORLD VS 1984**

Datensouveränität:
Warum Europa nicht
besser als China ist

56

**»WIR BRAUCHEN
AUCH IN ZUKUNFT
VIELE UNTER-
SCHIEDLICHE,
IDENTITÄTEN«**

Jurist Viktor
Mayer-Schönberger
im Interview

60

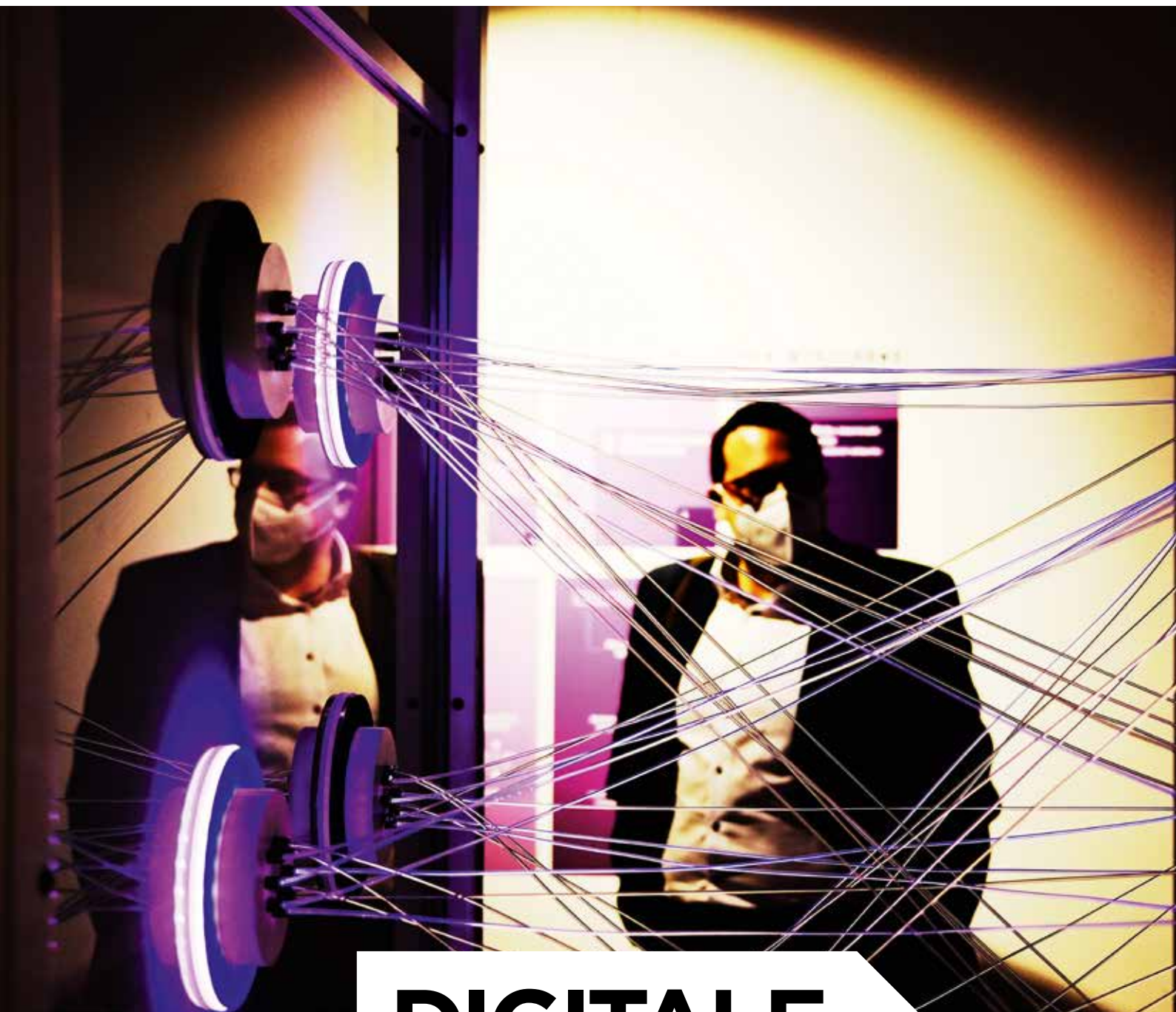
**»IDENTITÄT
IST UND BLEIBT
ETWAS
INDIVIDUELLES«**

Philosophin und
Autorin Lena Pint im
Gespräch

64

**»MASCHINEN
FÜHREN (NOCH)
KEIN LEBEN«**

Philosoph Konrad Paul
Liessmann im Interview



DIGITALE IDENTITÄT: VIELE WEGE, EIN ZIEL

Zentral vs. dezentral, private Initiativen gegen die staatliche Lösung: Zugänge zur „Digitalen Identität“ gibt es viele. Offen ist, wer sich letztlich durchsetzen wird. Eine Blick auf den Status quo in Österreich.

WIE ES UM DIE DIGITALE IDENTITÄT
IN ÖSTERREICH STEHT

TEXT OLIVER JANKO



Eine simple Plastikkarte bestimmt in der analogen Realität über Einlass oder Abweisung, über den Patientenstatus oder darüber, wem Konten oder Flugtickets zugewiesen werden. Wer zum Arzt muss, weist sich mit der eCard aus, wer fliegen will, mit dem Reisepass und in Bus, Bahn und Auto wird die jeweilige Plastikkarte als Ausweis gezücht, wenn die Kontrollinstanzen das fordern. Aber auch im Internet sind die physischen Identitätsnachweise (noch) unabdingbar: Neobanken und Krypto-Händler fordern nach wie vor Reisepässe oder Personalausweise zur Verifizierung der Identität per Videocall, Car-Sharing-Dienste scannen den Führerschein per App ein und versichern sich so, dass nur zugelassene Personen in die Autos steigen.

ID Austria statt Apple ID

Abseits dieser hybriden Verifizierungsformen - ein Onlinedienst, verifiziert wird aber mit einem physischen Offline-Medium - gibt es gerade im Internet keine einheitlichen Regeln und Normen, die den Identitätsnachweis regeln. Wer drei verschiedene E-Commerce-Handelsunternehmen nutzt, hat in der Regel drei Accounts, die wiederum zumeist per Mailadresse oder Google- beziehungsweise Facebook- oder Apple ID-Verifizierung erstellt werden. Die meisten kennen das: Diametral zur Anzahl an Diensten, die in Anspruch genommen werden, sinkt die Anzahl der gewählten Passwörter, sinkt das Maß an Kreativität, mit der die Kennwörter erdacht werden. Als Endergebnis bleibt dann oft die gleiche Kennung in verschiedenen Varianten - oder überhaupt ein Passwort für mehrere Dienste. Parallel dazu freut jede neue Anmeldung primär die US-Giganten, die fleißig Daten abziehen und das jeweilige Userprofil so laufend erweitern. Die Möglichkeit ist natürlich bequem, vor allem der EU aber schon länger ein Dorn im Auge - schließlich wissen Google, Apple, Facebook und Co dadurch ganz genau, wer was wann wo kauft.

Klare EU-Vorgaben

„Jedes Mal, wenn eine Website uns auffordert, eine neue digitale Identität zu erstellen oder uns bequem über eine große Plattform anzumelden, haben wir in Wirklichkeit keine Ahnung, was mit unseren Daten geschieht. Aus diesem Grund wird die Kommission demnächst eine sichere europäische digitale Identität vorschlagen. Eine, der wir vertrauen, und die Bürgerinnen und Bürger überall in Europa nutzen können, um alles zu tun, von Steuern zahlen bis hin zum Fahrrad mie-

ten. Eine Technologie, bei der wir selbst kontrollieren können, welche Daten wie verwendet werden“ - das erklärte Kommissionspräsidentin Ursula von der Leyen in ihrer Rede zur Lage der Union bereits am 16. September 2020. Die Lösung sollen sogenannte „digitale Identitäten“ - kurz eIDs - sein. So gut wie alle Staaten arbeiten an einer eigenen Lösung.

In Deutschland gibt es etwa vier Projekte, die „allesamt interoperabel sind und in den nächsten drei Jahren vorangetrieben werden“, erzählt Andreas Freitag, Consultant bei Jolocom und Experte im Themenbereich Self Sovereign Identity. Deutschland investiere „hohe zweistellige Millionenbeträge“ in die Projekte, 60 Unternehmen „mit Rang und Namen“ und 200 assoziierte Partner:innen würden an der Umsetzung einer nationalen Lösung arbeiten, die alle Aspekte abdeckt.

Zentral oder dezentral

Auch in Österreich wollen bei der eID mehrere Anbieter ein Stück vom Kuchen. Eine Zusammenarbeit der einzelnen Akteure und des Staates gibt es allerdings nicht. Letzterer arbeitet in Form des BMDW an der „ID Austria“ oder „Identity Austria“, daneben existieren verschiedene Lösungen aus der Privatwirtschaft, die ähnliches versprechen. Der größte Unterschied, etwas vereinfacht: ID Austria ist eine zentrale Lösung, also geschlossen und damit von außen kaum zu kontrollieren. Der „Lizenzgeber“ entscheidet somit auch über den Zugang zum System. Ein konkretes Beispiel: Die ID Austria als zentrale Lösung könnte in Zukunft beispielsweise in einer Wallet den Führerschein und die eCard digital beinhalten. Nicht möglich ist es aber, andere Dokumente in die Wallet zu laden - beispielsweise Rechnungen von Privatärzten oder das Uni-Zeugnis. Dafür müsste ID Austria zumindest ein entsprechendes Plugin anbieten, erklärt Freitag.

Dezentrale Lösungen setzen hingegen auf Open Source, was letztlich zur Folge haben soll, dass ein Wallet sämtliche Dokumente fasst - der Aktenordner wird digital. „Das digitale Identitätsdilemma, sprich die Unmengen an einzelnen digitalen Identitäten und Accounts, wird derzeit mit dem Einsatz zentraler digitaler Identitätslösungen gelöst“, erklärt Freitag. Als Beispiel dient hier die Anmeldeoption mit einem Social-Media-Account auf etwa Einkaufsplattformen. Freitag: „Der Identitätsanbieter verwaltet die Daten und hat das Recht diese zu ändern oder sogar zu löschen. Darüber hinaus hat er die Informationen wo und wann die Daten verwendet werden.“ Dezentrale digitale Identitäten seien indes unter der Kontrolle ihrer Nutzer:innen und würden von keiner zentralen Instanz verwaltet oder kontrolliert, beschreibt Freitag die gegensätzliche Variante. Zwei Ansätze und noch mehr einzelne Lösungen also: Wer gewinnt den Wettlauf um die digitale Identität? Oder lässt der Markt ohnehin verschiedene Zugänge zu? ►

»Mit der ID Austria ist ein verlässlicher, rechtlich geregelter, staatlich verantworteter Identitätsnachweis auch in der elektronischen Welt möglich. Dieser kann für digitale Services der Verwaltung ebenso eingesetzt werden wie für Services in der Wirtschaft.«

► **„Vertrauenswürdige Instrument“**

„Es steht der Privatwirtschaft natürlich frei, eigene Lösungen zu entwickeln und zu akzeptieren“, sagt Peter Kustor, Abteilungsleiter in der Digitalisierungssektion im Bundesministerium für Digitalisierung. Mit der Identity Austria bietet der Staat ein „sicheres und vertrauenswürdige Instrument“ an, das umfassend genutzt werden könne. Durch die „staatliche“ Ausstellung und die behördliche Identitätsprüfung, die der Ausgabe zugrunde liege, sei gewährleistet, „dass tatsächlich die Person hinter der elektronischen Identität steht, die dies behauptet“. Kustor: „Damit ist ein verlässlicher, rechtlich geregelter, staatlich verantworteter Identitätsnachweis auch in der elektronischen Welt möglich. Dieser kann für digitale Services der Verwaltung ebenso eingesetzt werden wie für Services in der Wirtschaft.“ Was fehlt: Services von Privatunternehmen, Privatärzten, Bildungseinrichtungen oder Behörden, die schlichtweg noch nicht digitalisiert sind.

Die Sache mit dem Führerschein

Gerade in Sachen Verwaltung sind die nächsten Digitalisierungsschritte auch unabdingbar. Das Paradebeispiel: Der digitale Führerschein soll - entgegen anderslautender Ankündigungen - nun doch erst 2022 Einzug halten. Dabei kostet langsame Digitalisierung bares Geld: Einer Studie von McKinsey zufolge könnte der Einsatz digitaler Technologien alleine die Gesundheits- und Versorgungskosten in Österreich um 14 % jährlich senken - in absoluten Zahlen etwa 4,7 Milliarden Euro. Alleine die Umstellung auf papierlose Datenverarbeitung soll demnach im Gesundheitswesen bis zu 900 Millionen Euro Einsparungspotenzial aufweisen.

Der Fahrplan für Österreich scheint auch darum klar: Statt zur Bezirkshauptmannschaft marschieren zu müssen, sollen Amtswege weitestgehend digital vonstatten gehen. Die Schwierigkeit: Wenn Hans Huber seinen Hauptwohnsitz ummelden will, muss sichergestellt sein, dass es sich bei der Person auch tatsächlich um Hans Huber handelt. Was braucht der Staat also? Im besten Falle eine Art „Generalschlüssel“, wie die

„Süddeutsche Zeitung“ die digitale Identität einmal bezeichnete. Das öffnet im Umkehrschluss aber auch potenzielle Einfallstore für Verbrecher - und wirft erst recht die Frage auf, ob der staatlichen Lösung oder der privatwirtschaftlichen Lösung mehr Vertrauen geschenkt werden sollte. „Meiner Meinung wird sich SSI durchsetzen, da es ein einheitlicher Standard ist, keiner Firma gehört und keine Systembrüche zwischen Silosystemen bestehen“, erklärt Freitag. Er setzt auf eine Wallet, „in die du Credentials aus verschiedenen Ländern rein legen kannst und verwaltest“.

ID Austria statt Handysignatur

Die ID Austria geht in eine andere Richtung, sie soll die lange Zeit ungeliebte Signatur ersetzen und als Silo-Lösung vor allem für Verwaltungsanliegen herangezogen werden. Peter Kustor: „Die Identity Austria ist eine Weiterentwicklung der Handy-Signatur. Auch mit Blick auf die vergangenen Monate sehen wir die Entwicklung der Handy-Signatur sehr positiv und erwarten weitere Zuwächse.“ Die Möglichkeit mittels Handy-Signatur auf den Grünen Pass zuzugreifen, habe einen „regen Zustrom“ ausgelöst. Mehr als 2,6 Millionen aktive Handy-Signatur-Nutzer:innen in Österreich soll es mittlerweile geben.

Keine Anwendung ohne Pandemie

Davor war die Handysignatur von A-Trust allerdings nicht unbedingt der Weisheit letzter Schluss. Noch im Jahr 2019 gaben laut Statista nur rund 38 Prozent der befragten Österreicher zwischen 18 und 34 Jahren an, im Besitz einer Handy-Signatur/Karte mit aktivierter Bürgerkartenfunktion zu sein. Das mag auch daran liegen, dass A-Trust „komplett zentral“ verwaltet ist und im Prinzip einsehen kann, was die Nutzerin oder der Nutzer in der App machen. „Melde ich mich bei der SVA an, gibt es einen Eintrag in der Datenbank“. Das sieht Freitag skeptisch: „Zwar sagt A-Trust, sie schauen derartige Daten nicht an, aber das wissen wir letztlich nicht. Das ist keine Zero-Trust-Architecture.“ Die ID Austria soll die lange Zeit ungeliebte Signatur künftig jedenfalls ersetzen. Die „Digitales Amt“-App wird - sobald flächendeckend ausgestattet - die Anmeldung ausschließlich

über die ID Austria zulassen. „Digitale Services der Verwaltung verwenden die staatlich gesicherten Identitätslösungen“, erklärt Kustor. „Nur bei diesen ist die eindeutige Identität auch umfassend gewährleistet und die Verantwortlichkeit für die Identitätsfeststellung klar. Nach dem EU-Rechtsrahmen der eIDAS-Verordnung werden auch die offiziellen eIDs der anderen Mitgliedstaaten akzeptiert. Auch bei diesen handelt es sich um digitale Identitätsnachweise, für die der jeweilige Mitgliedstaat die Verantwortung und Haftung trägt.“ Er wählt einen plakativen Vergleich: „Das ist ähnlich wie bei der physischen Ausweiskontrolle: Wenn ein Identitätsnachweis bei einer Behörde erforderlich ist, dann wird die Behörde einen amtlichen Lichtbildausweis verlangen und akzeptieren und sich nicht mit beispielsweise einer Kundenkarte eines Einkaufszentrums oder einer Mitgliedskarte beim Fitnessclub zufriedengeben.“

EU-weite Lösung

Unternehmen stehe es aber frei, andere Identitätslösungen zu akzeptieren. „Diese anderen Lösungen müssen sich aber in puncto Sicherheit und Rechtssicherheit, Verlässlichkeit und Datenschutz mit der Identity Austria-Lösung messen lassen“, meint Kustor. „Identity Austria wird in Zukunft auch in den anderen EU-Staaten umfassend einsetzbar sein, weil der europäische Rechtsrahmen eine gegenseitige Anerkennung dieser staatlich gesicherten eID-Systeme vorsieht.“ Auch das sei ein Vorteil gegenüber Alternativlösungen aus privater Hand.

Unabhängig davon gibt es mittlerweile zahlreiche Ansätze für die digitale Identität, in Österreich arbeiten einige Unternehmen an eigenen Anwendungen und Apps. International sind es noch deutlich mehr. Das wohl prominenteste Beispiel: „ID2020“, ein Konsortium, bestehend aus Unternehmen wie Microsoft oder Accenture, unterstützt von der US-Regierung. Auch heimische Lösungen sind aber erfolgreich. Mit younix hat das Tochter-Startup der Österreichischen Staatsdruckerei sogar bereits erste Kunden an Land ziehen können. Das Fürstentum Liechtenstein setzt auf die younix-Lösung MIA. Auf Seite 14 stellen wir Ihnen Unternehmen und Lösungen vor, die im Themenbereich „digitale Identität“ arbeiten.

Digitale Kopie

Die „Echtheit einer Person oder Sache“, die „völlige Übereinstimmung mit dem, was sie ist oder als was sie bezeichnet wird“ - das versteht der Duden offiziell als „Identität“ - zumindest in der klassischen Definition. In der Psychologie beschreibt der Terminus die als „Selbst“ erlebte „innere Einheit einer Per-

son“. Was die digitale Identität meint, ist also nichts anderes als eine digitale Kopie einer analog realen Person. Google, Facebook, Apple und Co versuchen das gewissermaßen seit Jahren - allerdings über den Umweg der Datensammelei. Was verraten wird, wird gesammelt und letztlich zu einem digitalen Profil zusammengesetzt.

Genau das soll künftig mit staatlichen und nationalen privatwirtschaftlichen Identity-Lösungen verhindert werden. Wer sich ausweisen will, soll das zumindest im Wissen machen, dass die bereitgestellten Daten nicht auf US-Servern herumliegen - wenn schon zentral gespeichert wird, zumindest im Land, vereinfacht ausgedrückt.

Dezentraler Best Case

Geht es nach Andreas Freitag, reicht aber auch das nicht. Er fordert Dezentralität: „Wenn der Staat Reisepässe ausgibt, ist das ja auch dezentral. Er weiß nicht, wann der Pass verwendet wird und wer ihn sieht.“ Das soll auch mit der digitalen Identität so sein. Freitag geht sogar noch einen Schritt weiter. Bei dezentralen Systemen müsse nur gezeigt werden, was relevant sei. „Ich habe eine App und zeige nur die Informationen her, die ich brauche.“ Der „Grüne Pass“ beispielsweise wäre aus seiner Sicht nur ein weiterer Nachweis in einer dezentralen Plattform mit den notwendigen Informationen. „Kein Impfdatum, kein Impfstoff. Ich zeige das beim Wirt her - und was interessiert den, dass ich zwei Mal mit Astra geimpft worden bin?“ Auch werde der Personalausweis in der Gastro kaum verlangt. „Ist die eID mit dem Grünen Pass verknüpft, ist das egal - es muss nicht einmal der Name angezeigt werden und trotzdem ist sicher, dass beide Variablen - also die Identität und der Impfstatus - zusammenpassen.“

Viele Ansätze also, offen ist nur, wer sich letztlich durchsetzt und ob die zahlreichen Player den angesprochenen Kuchen nicht ungenießbar machen, anstatt sich nur ein Stück davon zu schnappen. Wer letztlich erst recht wieder fünf verschiedene digitale Identitätslösungen verwenden muss, um sich überall anzumelden, wird die Vorteile tendenziell nicht wahrnehmen. Ob die verschiedenen Wege schließlich in einer Ausfahrt münden, wird sich zeigen. Andreas Freitag bedient ein Zitat von Stefan Raab: „Vorne ist da, wo sich keiner auskennt.“ Bleibt zu hoffen, dass die Richtung stimmt. ▀

Die wichtigsten Begriffe:

SSI

Self Sovereign Identity oder „Selbstbestimmte Identität“. Bedeutet, dass eine Person (oder Organisation) eine digitale Identität erzeugen und diese kontrollieren darf, ohne, dass eine zentrale Partei das erlauben muss. Inkludiert auch die eigene Datenhoheit.

AUTHENTIFIZIERUNG

Der Prozess der Überprüfung einer Identität.

VERIFIZIERUNG

Nachweis, dass Sachverhalt wahr ist - dass die Identität übereinstimmt.

MASSEN- ÜBERWACHUNG IN EUROPA

„THE RISE AND RISE OF BIOMETRIC
MASS SURVEILLANCE IN THE EU“



Ein Bericht mit dem Titel „The Rise and Rise of Biometric Mass Surveillance in the EU“ der EDRI (European Digital Rights) kommt zu einem bedenklichen Ergebnis: In den untersuchten Staaten Deutschland und den Niederlanden werden biometrische Überwachungssysteme bereits „wiederholt aus nichtigen und unverhältnismäßigen Gründen“ eingesetzt. Auch in Österreich kommt die automatisierte Gesichtserkennung in Ermittlungen des Bundeskriminalamts zum Einsatz. Die Software wurde laut dem BMI bei Atos IT Solutions mit dem Subunternehmen Cognitec Systems GmbH zu einem Anschaffungspreis von 448.813,20 Euro erworben.



DAS RICHTIGE SETUP SCHAFFEN FÜR DIGITALE SOUVERÄNITÄT

MARIANA KÜHNEL, STELLVERTRETENDE
GENERALSEKRETÄRIN DER
WIRTSCHAFTSKAMMER ÖSTERREICH

Das Internet als Fenster zur Welt hat uns gerade während der Lockdown-Phasen ermöglicht, am alltäglichen Leben teilzuhaben. Doch wie werden reale Personen im virtuellen Raum vertreten? Mit ihrem digitalen „Ich“ als digitalem Ausweis, rechtskonform und sicher. Mittlerweile können in Österreich über 230 Services aus der öffentlichen Verwaltung digital erledigt werden - an 365 Tagen im Jahr. Die kostenlose Handy-Signatur, zählt im September 2021 beinahe drei Millionen aktive User.

Auch die Wirtschaft baut ihre digitalen Dienste laufend aus, derzeit sind über 4000 Anwendungen digital durchführbar. Wer eine Wohnung kaufen möchte, muss per se nicht mehr ins Immobilienbüro; um einen Deal mit einer spanischen Firma abzuschließen, steigt man nicht mehr ins Flugzeug, sondern fertigt den Vertrag einfach digital ab. Den Rechts-

rahmen dazu liefert unter anderem die eIDAS-Verordnung und stellt sicher, dass die digitale Identität europaweit anerkannt wird.

Die Möglichkeiten der digitalen Identität sind dabei noch lange nicht ausgeschöpft. Für Europa bedeutet das: Wenn es um Daten-Souveränität, um digitale Souveränität geht, müssen wir mutiger werden, die Innovationen sind da. Jetzt geht es darum, digitale Geschäftsmodelle zu ermöglichen bzw mit einer breit angelegten Digitalisierungsstrategie Chancen zu schaffen. Es geht um das richtige Setup für einen selbstbestimmten Umgang mit digitalen Innovationen. Und es geht um Technologiesouveränität, die dafür eine wichtige Voraussetzung ist. Digitale Ökosysteme sind kein Selbstzweck, sondern eine kritische wirtschaftliche Größe, die maßgeblich sind für Wertschöpfung und Arbeitsplätze. ▀

»Mit der digitalen Identität haben wir die Chance, die Verlässlichkeit, Sicherheit und Selbstbestimmtheit im digitalen Alltag ein Stück weit zu verbessern. SignD verfolgt das Ziel, eine Vielzahl von nützlichen Diensten mithilfe von Trusted Services möglich zu machen und dabei darauf zu achten, die digitale Souveränität des Einzelnen sicher zu stellen.«

BERNHARD REITERER,
CEO SIGND IDENTITY

*»Initiativen wie die eID können in Zukunft die digitale Identität für europäische Bürger*innen abbilden. Diese Identitäten können nicht nur für die Authentifizierung bei Bürger*innenservices, sondern auch für das rechtsgültige qualifizierte Signieren, zum Beispiel auf Plattformen wie Sprooff verwendet werden.«*

CLEMENS BRUNNER,
CEO SPROOFF

»Die digitale Identität ist das Fundament für vertrauenswürdige Digital-Services. Einerseits gewährleistet die digitale Identität einen einfachen und konsistenten Zugang zu meist öffentlichen Einrichtungen, andererseits wird dadurch garantiert, dass der User über die Datenhoheit verfügt. Aus Perspektive von Leftshift One ist diese Entwicklung daher unabdingbar.«

PATRICK RATHEISER,
CEO LEFTSHIFT ONE

»Die Einführung der ID Austria, der Weiterentwicklung der Handy-Signatur, ist ein wichtiger Schritt um Österreichs Spitzenposition in Sachen digitaler Signatur weiter zu stärken. Vor allem werden aber Bürgerinnen und Bürger von ihr und den dadurch entstehenden neuen digitalen Services, wie bspw. dem digitalen Führerschein, profitieren: Die ID Austria bringt noch mehr Komfort unter höchstem Datenschutz.«

DR. MARKUS VESELY,
CEO A-TRUST

»Wünschenswert wäre die Abhängigkeit von bekannten zentralen Ansätzen wie „Single-Sign-On via Google, Facebook, Apple, Microsoft, Amazon“ zu reduzieren. Als besonders viel versprechende Ideen erweisen sich hierbei dezentrale Architektur Ansätze und das Konzept der „Self-Sovereign Identity - SSI«

EDUARD PRINZ, ÖSTERREICHISCHE FOR-
SCHUNGSFÖRDERUNGSGESELLSCHAFT
MBH FFG

»Mit einem offenen Zugang zur digitalen Identität erreichen wir mehr Transparenz und schnellere Abwicklungen im alltäglichen Leben. Stellen wir uns einfach vor, wir können mit nur einem Login E-Bikes mieten, Kleidung online tauschen und alle offenen Rechnungen per Klick überweisen. Wir in Europa sollten Vorreiter werden und das volle Potenzial der Technologie aufzeigen.«

KAMBIS KOHANSAL VAJARGAH,
WKÖ HEAD OF STARTUP-SERVICES

BUSINESS

DAS GESCHÄFT HINTER DEN DATEN





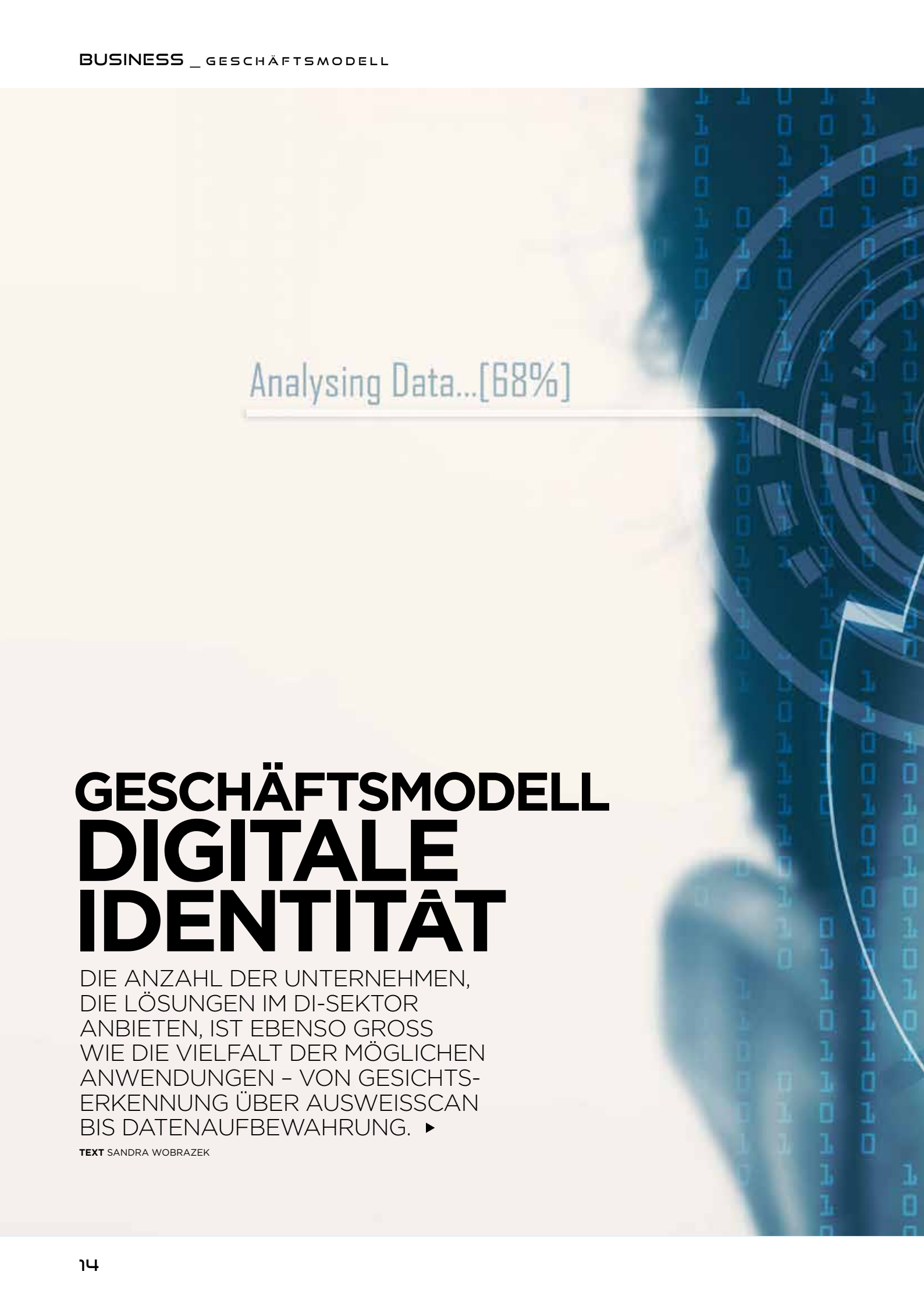
Europaweit entwickeln Unternehmen innovative DI-Produkte für verschiedenste Branchen. Die Bandbreite reicht von digitalen Ausweisen auf dem Smartphone bis zu virtueller Unternehmenssicherheit.

Damit sich Privatpersonen ebenso wie Unternehmen und deren Mitarbeiter:innen sicher im Netz bewegen können, sind verschiedenste Voraussetzungen notwendig. Eine der wichtigsten: Durchdachte Systeme und Apps, die digitale Vernetzung ermöglichen und dabei die höchstmögliche Sicherheit von Daten gewährleisten.

Im Bereich digitaler Ausweise gibt es europaweit bereits ein umfassendes Portfolio an sicheren Lösungen. Die Wiener Younix Identity hat etwa mit der „My Identity App“ (MIA) ein System für integriertes Identitätsmanagement geschaffen, das physische Ausweisdokumente mithilfe einer plattformunabhängigen Smartphone-App in digitale Dokumente transferiert. Auch bei der selbstbestimmten Datenverwaltung gibt es bereits tragfähige Modelle: Mit dem Login-System „MeineSicherID“, basierend auf dem Self-Sovereign-Identity-Prinzip (SSI), sollen Nutzer selbst entscheiden, mit wem sie welche ihrer persönlichen Daten teilen, indem auch diese auf dem eigenen Smartphone abgespeichert und bei Bedarf geteilt werden.

Dabei nutzen in der Branche immer mehr Entwickler die hohen Sicherheitsstandards aus dem Bankenbereich. Die ich.app, ein Produkt der PSA, etwa ist die digitale Identität der österreichischen Banken. Sie bietet die Möglichkeit, von der Bank geprüfte Daten im Netz als Identitätsnachweis zu nutzen und so unkompliziert Zugänge zu verschiedensten Services zu bekommen. Die European netID Foundation wiederum möchte mit dem Single Sign-on eine unabhängige und datenschutzkonforme Alternative zu den Login-Diensten der großen US-Konzerne bieten. Das Ziel: Die Nutzer:innen sollen die Kontrolle über ihre Daten behalten und transparent über deren Verwendung entscheiden können. Neben der privaten Dokumentenverwaltung ebenso ein großes Thema: Digitale Identität im Unternehmenskontext. Die von VID-International entwickelte VID-Card ist ein dezentrales System für die Verwaltung von Unternehmen, Mitarbeiter:innen und unternehmensübergreifende Berechtigungen im B2B-Bereich. ▀

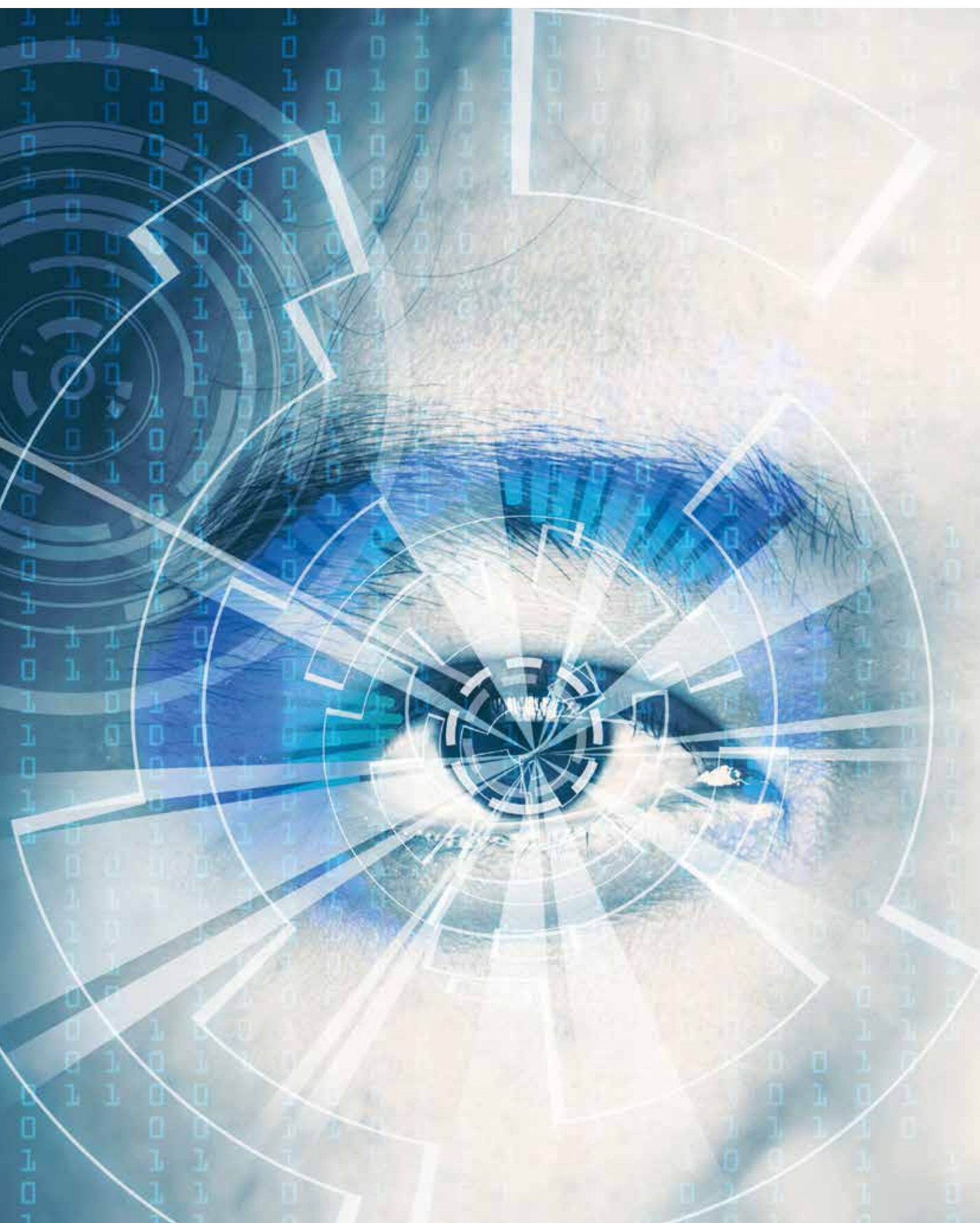
Analysing Data...[68%]



GESCHÄFTSMODELL DIGITALE IDENTITÄT

DIE ANZAHL DER UNTERNEHMEN,
DIE LÖSUNGEN IM DI-SEKTOR
ANBIETEN, IST EBENSO GROSS
WIE DIE VIELFALT DER MÖGLICHEN
ANWENDUNGEN - VON GESICHTS-
ERKENNUNG ÜBER AUSWEISSCAN
BIS DATENAUFBEWAHRUNG. ►

TEXT SANDRA WOBRAZEK





Anyline setzt seit kurzem auf biometrische Gesichtsverifikation und „Liveness-detection“.

ANYLINE

„Innovation ist nichts ohne adäquate Schutzmaßnahmen. Bei Anyline ist es daher Standard, dass Daten am Gerät und offline verarbeitet werden.“

ALEXANDER LOIDOLT
SVP Enterprise Business
Anyline



Seit kurzem erlebt er einen Boom an innovativen Entwicklungen – der Markt für Lösungen in Sachen Digitaler Identität (DI). Auch in Österreich wurden und werden, im B2B- ebenso wie im B2C-Sektor, innovative und praktikable Lösungen entwickelt, die es möglich machen, dass Daten im Netz mit größtmöglicher Sicherheit verwendet werden.

Eines der aktuell bekanntesten DI-Projekte: ID Austria, mit der man sich online ausweisen und so digitale Services in Verwaltung und Wirtschaft nutzen und Geschäfte tätigen kann. Aktuell noch in der Pilotphase, soll sich das Service des Bundesministeriums für Digitalisierung und Wirtschaftsstandort (BMDW) und des Bundesministeriums für Inneres (BMI) als eine Weiterentwicklung von Bürgerkarte und Handy-Signatur etablieren.

Digitale Identitätslösung

Bereits umgesetzt wurde MIA (My Identity App), die weltweit erste vollintegrierte, digitale Identitätslösung: MIA, ein Produkt der younix Identity AG, einer Tochter der Österreichischen Staatsdruckerei, kombiniert als Smartphone-App digitale Ausweise mit einer sicheren und modernen eID-Lösung. In der App werden zwei der wichtigsten Bereiche von digitalen Identitäten abgedeckt. Auch

deshalb ist MIA in zwei europäischen Ländern bereits im Echtbetrieb-Einsatz, wie Mag. Lukas Praml, Geschäftsführer Österreichische Staatsdruckerei GmbH und Vorstand younix Identity AG, erklärt.

Seiner Meinung nach die derzeit größte Herausforderung ist der umfassende Schutz von sensiblen Identitätsdaten. „Eine moderne digitale Identität darf ihre Userinnen und User im alltäglichen Gebrauch nie durch Sicherheitsvorkehrungen einschränken, sondern muss einfach und rasch nutzbar sein. Gleichzeitig muss im Hintergrund zu jedem Zeitpunkt für umfassende Sicherheit gesorgt sein.“ In der younix Identity fließen Überlegungen zur Sicherheit ab dem ersten Tag in die Entwicklung ein. „MIA hat im Echtbetrieb bewiesen“, sagt Lukas Praml, „dass wir die User-Erwartungen erfüllen können. Es ist unser Anspruch, immer die höchstmögliche Qualität zu liefern – daher entwickeln und verbessern wir unsere Lösungen laufend weiter.“

Datensouveränität

Die Grundidee hinter MSID (Meine sichere ID) wiederum ist ein dezentrales Daten-Ecosystem, basierend auf dem Self-Sovereign-Identity-Standard (SSI), in dem identitätsbe-

zogene Daten ausgetauscht werden. Kreiert von verschiedensten österreichischen Unternehmen und Institutionen (wie dem Handelsverband, der APA und A1) steht im Mittelpunkt vom MSID der Mensch als „Owner“ seiner Daten, der alleine entscheidet, wer welche Daten zu welchem Zweck erhält.

„Damit wandert die Datenhoheit von Unternehmen und deren Silos, die diese Daten als Geschäftsmodell verwerten, zu den Bürgerinnen und Bürgern und entspricht zu 100 Prozent der DSGVO“, erläutert Gerhard Krammer von der Agentur Business Design.

Dabei kann in MSID jede Art von Daten bereitgestellt werden – von KYC-Daten von Banken und Ausbildungszertifikaten bis hin zu Loyalty-Programmen von Handelsketten. „Es gibt keine zentralen Stellen, die über den Austausch der Daten informiert sind. Als Betreiber steht der gemeinnützige Verein für digitales Vertrauen und damit keine Gewinorientierung dahinter.“

Multifunktionale Daten

Auch Daten aus dem Bankenwesen dienen zunehmend als Basis für neue ID-Lösungen, wie sich am Beispiel der ich.app, einem Produkt der PSA – Payment Services Austria, zeigt, die 2022 ihre Marktreife erlangen wird.



MIA

„MIA kombiniert als Smartphone-App digitale Ausweise mit einer sicheren und modernen eID-Lösung.“

LUKAS PRAML

Geschäftsführer Österreichische Staatsdruckerei GmbH & Vorstand younixx Identity AG

MeineSichereID

**DIE GRUNDIDEE VON MEINESICHEREID:
DIE DATENHOHEIT VON UNTERNEHMEN
WANDERT ZU DEN BÜRGERINNEN
UND BÜRGERN.**

Die von der Bank geprüften Daten eines Kunden oder einer Kundin können in der ich.app als Identitätsbestätigung für verschiedenste Services genutzt werden. Der Login im Onlineshop ist damit ebenso möglich wie die Registrierung im Hotel oder die Authentifizierung bei Online-Services.

Nicht nur das Ausweisen, auch die Überprüfung der Identität spielt eine entscheidende Rolle im weiten Feld der DI. Doch auch hier sind bereits tragfähige Lösungen auf dem Markt: paybox Ident ermöglicht es Unternehmen bei Einkäufen, Registrierungen oder Verträgen, die Identität der Kundinnen und Kunden online zu überprüfen – innerhalb weniger Sekunden, rechtskonform und vollautomatisch. Dabei wird auf eine einheitliche Plattform gesetzt, die mehrere Ident-Verfahren miteinander kombiniert und in bestehende Websites und Online-Shops integriert werden kann.

Schlüssel in der Online-Welt

Sowohl für Unternehmen als auch für Nutzerinnen und Nutzer gedacht ist Swilox. Die App der Linzer Swilox GmbH löst das



MIA (My Identity App) ist die weltweit erste vollintegrierte digitale Identitätslösung.



- Problem dutzender verschiedener Identitäten im Netz, indem sie das Handy zum Schlüssel in der Online-Welt macht – ohne Username oder Passwort. Der Zugriff auf den eigenen Account soll dadurch einfacher, schneller und sicherer werden. Mittels eines Klicks am Handy ist man angemeldet, am PC in der Arbeit ebenso wie am Familien-Tablet oder am eigenen Handy. „Die Anzahl der digitalen Geräte, die wir im täglichen Leben nutzen“, sagt Swilox CEO Dr. Alexander Fried, „wird immer größer: Notebook, Handy, Tablet, aber auch Smart TV oder digitale Self-Service-Kioske. Überall wollen wir auf unsere eigenen Daten Zugriff haben oder Aktionen persönlich autorisieren. Swilox hilft durch ein einfaches Konzept: Ein Scan, ein Klick, erledigt.“

Blockchain-Technologie

Ergänzend entstehen mehr und mehr DI-Lösungen in Kooperationen zwischen Forschungseinrichtungen und Unternehmen. In einem mehrjährigen Forschungsprojekt des Startups VID International mit dem Austrian Blockchain Center wurden die Erstellung, Verwaltung und der Betrieb von Identitätsmanagement bei führenden Blockchains analysiert – und die Resultate in eine Applikation mit einfacher Usability übersetzt: der VID-Card.

Die VID-Card funktioniert unabhängig von spezifischen Blockchains („agnostisch“) und zeichnet sich durch besonders benutzerfreundliche Interaktion aus, wie Ing. Daniel Gosterxeier, CEO VID International, erklärt. „Eines der Hauptmerkmale ist die Möglichkeit die Accounts (Identität) bei Verlust von Passwörtern (Credentials) wiederherstellen zu können. Die Applikation bietet Integrationen und Einsatzmöglichkeiten in internen und externen Unternehmensprozessen und ermöglicht Firmen kostenoptimiert zu arbeiten. Ein virtuelles Rollensystem kann Strukturen im Unternehmen abbilden und somit Abläufe im Unternehmen weiter zeitbezogen digital verbessern.“

Ausweis-Scan

Doch es ist nicht nur die Verwaltung der Daten, die DI-Unternehmen beschäftigt, auch das Scannen von Ausweisen und Formularen spielt eine entscheidende Rolle, wenn es um virtuelle Identitäten geht. Das Startup Anyline ermöglicht es dank Mobile Optical Character Recognition (OCR) seinen Klientinnen und Klienten, hunderte von unterschiedlichen Ausweisen, wie Reisepässe, Führerscheine, Personalausweise und viele Variationen von Visa, mit einem mit einer Kamera ausgestatteten Smartphone, Tablet oder Notebook zu scannen. Anyline ist deshalb auch weltweiter DI-Partner von Regierungen, Strafverfolgung (inklusive der österreichischen Polizei) und Finanzinstituten.



SWILOX

„Studien zeigen: Viele Nutzer überfordert es, die eigene Identity mittels Username und Passwort nachzuweisen – denn wir haben schon so viele Passwörter.“

ALEXANDER FRIED
CEO Swilox





VID CARD

„Eines der Hauptmerkmale der VID-Card ist die Möglichkeit die Accounts bei Verlust von Passwörtern wiederherstellen zu können.“

DANIEL GOSTERXIER
CEO VID-International



VID DESIGN EVOLUTION

VID EVOLUTION

VID-CARD IST EINE KOMPLETT DIGITALE LÖSUNG FÜR DIE VERWALTUNG VON UNTERNEHMEN, MITARBEITERINNEN UND MITARBEITERN UND UNTERNEHMENSÜBERGREIFENDEN BERECHTIGUNGEN.

In den letzten zwei Jahren wurden die ID-Scanning-Fähigkeiten um zusätzliche Verifikationstechnologien erweitert. „Dazu gehören das NFC-Chip-Lesen, welches verwendet werden kann, um gefälschte ID-Dokumente zu identifizieren oder auch biometrische Gesichtsverifikation und „Liveness-detection“, sagt Anyline-Sprecher Alexander Loidolt. „Im Gegensatz zu Alternativen, die IDs in der Cloud abwickeln, garantieren wir, dass sämtliche Daten, die während eines ID-Scans erfasst werden, auf dem Smartphone der Besitzerin oder des Besitzers bleiben. Somit vermeiden wir die Gefahr, dass Daten von einer dritten Partei abgehört und aufgefangen werden.“

Datenschutz und Datensicherheit

Auch europaweit und länderübergreifend ist die digitale Identität ein großes Thema. Die European netID Foundation bietet den Nutzerinnen und Nutzern mit Single Sign-on eine unabhängige und datenschutzkonforme Alternative zu Login-Diensten der US-Konzerne. Publisher, Onlineshops und Website-Betreiber haben mit den Marktlösungen netID Professional und netID Enterprise die Möglichkeit, ihren Nutzern die Verwaltung ihrer Privatsphäre-Einstellung übersichtlich und einfach zu gestalten. „Basierend auf den hinterlegten Einwilligungen können“, sagt Achim Schlosser, CTO & Interims-CEO der European netID Foundation, „ohne Third-Party-Cookies Device-übergreifend personalisierte Werbekampagnen ausgespielt werden. Grundlage ist das transparente Einwilligungsmanagement sowie der stabile netID Identifier.“

Zukünftige Herausforderungen der Branche, davon ist Achim Schlosser überzeugt, lie-

gen in Datenschutz und Datensicherheit – vom digitalen Personalausweis im Netz bis zum Login beim E-Commerce-Shop oder dem Onlinemedien-Angebot: „Digitale Identität findet sich in vielen Bereichen. Marktlösungen sollten ein breites Spektrum an Anwendungsfällen abdecken, damit Nutzer so wenige Systeme wie möglich anwenden müssen. DSGVO, e-Privacy-Verordnung und das TTDSG, all diese Gesetze und Verordnungen gilt es zu beachten“. //



NETID

„Marktlösungen sollten ein breites Spektrum an Anwendungsfällen abdecken, damit Nutzerinnen und Nutzer so wenige Systeme wie möglich anwenden müssen.“

ACHIM SCHLOSSER
CTO & Interims-CEO der European
netID Foundation

NETID_ENID

Die European netID Foundation bietet mit dem Single Sign-on eine unabhängige und datenschutzkonforme Alternative zu den Login-Diensten der US-Konzerne.

BANKEN, BOTS & DIGITALE BÖRSEN

Online-Schnellkredit, ETF, Tesla-Aktie, Bitcoin - zwischen einem eifrigen Online-Konsumenten und einem heißen neuen Finanzprodukt steht in der Regel eines: die digitale Ausweiskontrolle. In der Regel verbringen Nutzer:innen zwischen fünf und zehn quälende Minuten in Video-Calls, in denen sie dem netten Mitarbeiter des brandneuen Fintechs ihren Ausweis über die Smartphone-Kamera entgegen halten.

Bald sollen es nur mehr zwei, drei Minuten sein, und in absehbarer Zukunft wird das Identifizierungsverfahren in Trading-Apps, bei Online-Shops oder beim Krypto-Händler nur mehr Sekunden dauern. Grund dafür ist die rasante Entwicklung, die Identity-Tech-Anbieter hinlegen. Bald werden nicht mehr Mitarbeiter:innen von Neobanken am anderen Ende der Leitung sitzen und Ausweise kontrollieren, sondern Künstliche Intelligenzen. Und auch die haben bereits ein Ablaufdatum. Denn wenn die Pläne der EU aufgehen, dann werden alle Bürger:innen eine digitale Wallet haben, von der er aus in Sekundenschnelle Banken, Versicherungen oder Exchanges auf seine lokal am Smartphone gespeicherte digitale Identität selektiv zugreifen lassen wird.

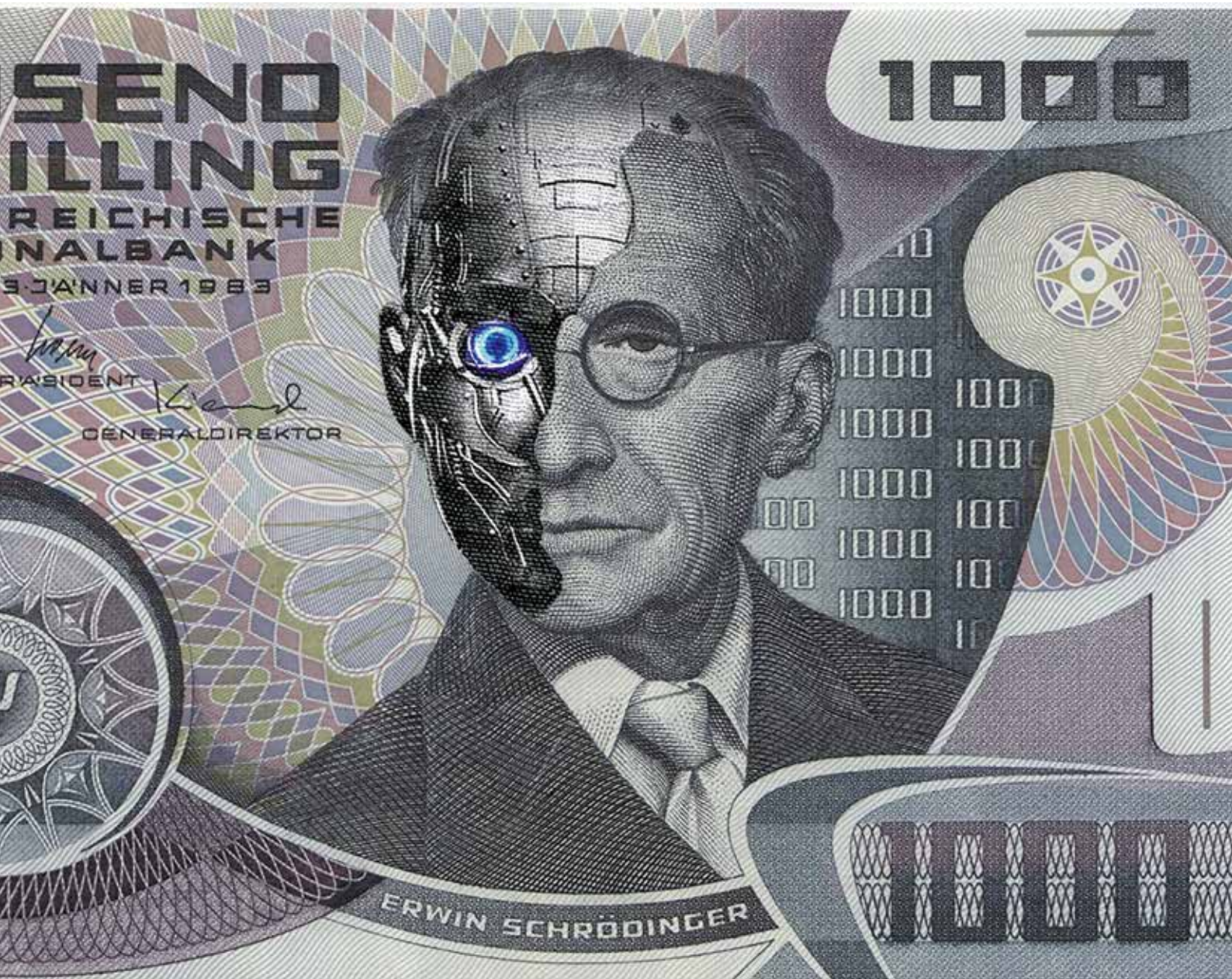
Fintechs treiben den Trend

„Initial waren die Fintechs ganz klar die Treiber dieses Trends, N26 etwa war einer unser ersten Kunden. Mittlerweile haben auch die klassischen Banken das erkannt und sind nachgezogen“, sagt Armin Bauer, Mitgründer und Managing Director Technology beim deutschen Identity-as-a-Service-Anbieter IDnow. Als Endkund:in merkt man es nicht, aber IDnow sorgt im Hintergrund bei zahllosen digitalen Finanzdienstleistungen dafür, dass sich Nutzer:innen den Richtlinien für Geldwäsche gemäß ordentlich identifizieren lassen können. Solarisbank, N26, Erste Bank, Holvi, Sparkasse, Raiffeisen Bank International, UBS - die Liste der Kund:innen ist lange und prominent besetzt, das Who is Who der europäischen Finanzbranche. Die Zeiten, in denen man beim Postbeamten mit dem Pass antanzen ►



Fintechs haben dafür gesorgt, dass digitale Identitätslösungen massentauglich wurden. Das könnte zum entscheidenden Vorteil des in der Digitalisierung rückständigen Europa werden.

TEXT JAKOB STEINSCHADEN ILLUSTRATION DAVID VISNJIC





»Digitale Identität ist der erfolgskritische Hebel, um Menschen zu helfen und zu schützen.«

DANIEL GOLDSCHIEDER
Gründer und CEO
bei yes.com

► musste, um ein Sparkonto zu eröffnen, sind längst vergessen. In Deutschland sind es laut Bauer mittlerweile gar 80 Prozent der Internetnutzer:innen, die schon einmal mit einem digitalen Identifizierungsverfahren in Kontakt kamen. Treiber der Entwicklung ist ganz klar die Fintech-Branche. Noch vor einigen Jahren hieß es oft, dass das Facebook-Konto das Non Plus Ultra sei, mittlerweile gilt aber das Bankkonto und die darin enthaltenen Transaktionsdaten als der Heilige Gral des Daten-Business. Nicht „Du bist, was dir gefällt“, sondern „Du bist, was du kaufst“, lautet das Motto. Und die Firmen, die auf diese Daten zugreifen wollen, müssen eben ordentliche Identifizierungsverfahren einsetzen.

Von Minuten zu Sekunden

Beschleunigt wird das Geschehen am Markt von weiteren Faktoren. „In den letzten 24 Monaten hat aus unserer Sicht das Social Distancing, einige regulatorische Anpassungen sowie technische Innovation einen Schub im Markt der Identitätslösungen bewirkt“, sagt Daniel Goldscheider, CEO und Mitgründer von yes.com. „Digitale Identität ist der erfolgskritische Hebel, um Menschen zu helfen und zu schützen. Wir haben die technischen Standards, für ein interoperables globales Identitäts-Netzwerk geschaffen. Was noch fehlt, ist der Wille zur gemeinsamen Kraftanstrengung.“

Das Schweizer Fintech sieht sich als einer der Vorreiter bei Digital Identity und hat sich als Partner der Banken positioniert. Um ein globales Identitätsnetzwerk zu kreieren, arbeitet yes.com mit internationalen Playern wie Adobe, Akoya, BankID, Disney, DocuSign, Santander und den Sparkassen zusammen. Schon jetzt macht yes.com die Identitätsbestätigung so einfach wie eine Überweisung, indem Nutzer:innen den direkten Datentransfer aus den Systemen der Bank an den anfragenden Partner (z.B. einen Online-Shop) auslösen können.

Embedded Finance

Solche extrem schnellen Identitätslösungen sind essentiell für Fintechs. Ein Beispiel ist Klarna, Europas größtes Fintech mit einer Bewertung von mehr als 45 Milliarden Dollar. Als „Buy Now Pay Later“-Unternehmen (BNPL) bieten die Schweden Händler:innen an, dass sie Rechnungskauf, Ratenzahlung und Rahmenkredite quasi auf Knopfdruck in ihre Online-Shops im Checkout integrieren.

Weil es dabei natürlich oft um große Summen und die Bonität der Kund:innen geht, muss Klarna in Sekundenschnelle eine Risikoprüfung durchführen und checken, ob der Käufer sich den Schnellkredit überhaupt leisten kann.

Dafür wird mittels interner (Kaufhistorie, Zahlungsverhalten) und externer Daten (z.B. Schufa) in Sekundenschnelle berechnet, ob ein Kunde, eine Kundin im Online-Shop überhaupt die Option erhält, den Kauf auf Raten machen zu können. „Wir haben entsprechende Präventions- und Scoring-Modelle, nach denen wir entscheiden, ob eine Zahlart einem Kunden überhaupt zur Verfügung steht“, so DACH-Klarna-Chef Thomas Vagner. Man sei eine „Kontrollinstanz“, die prüfen muss, wer sich etwas leisten kann - und wer eben nicht.

Kontrolleur AI

„Der Finanzsektor ist im Vergleich zu anderen Sektoren deutlich voran und macht immer noch den größten Teil unserer Kunden aus. Mittlerweile sehen wir aber, dass auch andere Sektoren nachziehen, etwa im Bereich der Versicherungen, im E-Health oder in der Mobility“, sagt Bauer. Dem entsprechend hart umkämpft ist auch der Markt. IDnow ist einer von mehreren Playern, die gerade dabei sind, den stark zersplitterten Markt mit zahlreichen lokalen Nischen-Playern aufzuräumen. Bauer: „Wir gehen davon aus, dass es in Europa fünf, sechs große Player geben wird und die heute extreme Fragmentierung verschwinden wird.“

Während heute noch das Video-Ident-Verfahren dominiert, wird bald AI werken. „Wir sind mit dem Video-Ident-Verfahren gestartet, hatten aber damals schon die Idee, das Ganze mit Künstlicher Intelligenz durchzuführen. Damals ging das noch nicht, aber heute geht es stark in Richtung KI-basiertes Identifikationsverfahren“, sagt Bauer. Dann wird zwischen einem App-Download und der Kontoeröffnung nur mehr zwei, drei Minuten stehen - und möglicherweise die eine oder andere Behörde.

„Es gibt immer noch Regulierungsbehörden, die denken, dass die Ausweiskontrolle ein Mensch, also ein:e Mitarbeiter:in oder am besten ein Beamter oder eine Beamtin machen muss, aber die Erkenntnis, dass KI viel genauer ist, setzt sich immer mehr

»Es gibt immer noch Regulierungsbehörden, die denken, dass die Ausweiskontrolle ein Mensch, also ein Mitarbeiter oder am besten ein Beamter machen muss, aber die Erkenntnis, dass KI viel genauer ist, setzt sich immer mehr durch.«

durch“, sagt Bauer. „Die Algorithmen sind dem Menschen heute deutlich überlegen. Ein gut trainierter Mensch hat eine Fehler-rate von zwei bis drei Prozent, unsere Algorithmen aber nur 0,3 Prozent, sind also zehn Mal besser.“

Algorithmen im Hintergrund

Und auch hier sind es wieder die Fintechs, die den Ton angeben. So setzt Coinbase, der börsennotierte, milliardenschwere Krypto-Händler aus den USA, die Technologie von Solarisbank (wiederum IDnow-Partner) ein, um Nutzer:innen innerhalb von Sekunden über ein Referenzkonto zu identifizieren. Ausweise in Kameras halten, das wird bald antiquiert wirken. Denn künftig werden Algorithmen die Identifizierung übernehmen.

„Dienstleister erwarten in digitalen Prozessen Antworten auf Fragen wie ‚Wer bist du‘, ‚erfülle du die Bedingungen‘, ‚bist du vertrauenswürdig/solvent genug‘ oder ‚Wie zahle ich‘“, sagt Goldscheider von yes.com. „Wer diese Fragen möglichst einfach, medienbruchfrei und grenzüberschreitend beantworten hilft, hat beste Chancen.“

Software, Algorithmen und Plattformen werden also unsere digitale Identität bestimmen. „Die Zukunft sehen wir ganz klar bei Digital Wallets. Heute sind Identverfahren transaktionsbasiert, man muss sich also etwa bei jedem Finanzinstitut neu identifizieren. Künftig aber wird es Digital Wallets geben, bei denen man sich einmal identifiziert und diese digitale Identität dann immer wieder für verschiedene Usecases verwenden kann“, sagt Bauer. Zentral dafür ist die „European Digital Identity“ (EDI), die die Grundlage für diese Digital Wallets schafft. Die Standardisierung soll dafür sorgen, dass man eine deutsche ID-App auch in Österreich verwenden kann, und sie soll es für verschiedene Zwecke ermöglichen, dass vom Fischerverein über die Universität bis zur Großbank jeder (und nicht nur Behörden) digitale Ausweise ausstellen kann.

Zwischen EU und GAFA

Das bedeutet am Ende nicht, dass sensibelste Nutzerdaten frei zwischen Banken, Neobroker und Krypto-Exchanges hin und her fließen werden. „Der Bürger soll die Kontrolle

über seine Daten bekommen und kann selbst bestimmen, mit wem er diese Daten teilen will. Wenn eine Bank eine Identifizierung braucht, dann schickt sie eine Anfrage an die Wallet des Bürgers, und der kann dort ablehnen oder freigeben, welche Daten die Bank sehen darf und welche nicht“, sagt Bauer. Eine noch ungeklärte Frage ist, wo die Daten sitzen werden. In den Apps der Anbieter, oder am Ende doch in den mobilen Betriebssystemen von Google oder Apple?

„Die Novelle der eIDAS (Verordnung über elektronische Identifizierung und Vertrauensdienste, Anm.) scheint aktuell Ansätze von Wallets stark zu begünstigen“, sagt Goldscheider von yes.com. „Das scheint auch die Position der GAFAs bzw. Hardware-Gatekeeper im Mobile-Bereich zu stärken.“ Digitale Wallets gibt es bei Google (Android) und Apple (iOS) bereits heute, auch wenn sie eher als digitale Ablage für Konzertkarten und Flugtickets starteten. Doch sie drängen immer stärker in Richtung offizieller Ausweise und in den Online-Banking-Bereich, wie die Beispiele von Google Pay und Apple Pay zeigen.

Europa im Vorteil

Doch europäische Anbieter wie IDnow sehen sich am Heimatkontinent trotzdem im Vorteil. Denn anders als bei Social Media ist der Finanzbereich stark durch europäische Firmen geprägt - unter anderem auch deswegen, weil US-Neobanken wie Chime oder US-Neobroker wie Robinhood lieber im riesigen Heimatmarkt bleiben und ihren europäischen Pendants die komplizierte Angelegenheit mit den 27 teilweise sehr unterschiedlichen Mitgliedstaaten überlassen. Außerdem: Die EU ist sehr viel strenger als die USA. Einige US-Anbieter sind am Alten Kontinent gar nicht erlaubt.

„Das europäische Umfeld ist sehr streng reguliert und hat hohe Anforderungen, und die Verfahren aus den USA sind hier gar nicht zugelassen. Deswegen tun sich US-Player hier sehr schwer. Chinesische Anbieter haben es noch schwerer, nicht nur wegen der Skepsis, sondern auch, weil dort andere Verfahren üblich sind“, sagt Bauer. „Große staatliche Massenüberwachungsdatenbanken sind in Europa nicht gerne gesehen.“



»Große staatliche Massenüberwachungsdatenbanken sind in Europa nicht gerne gesehen.«

ARMIN BAUER
Gründer und Managing
Director Technology bei
IDnow

»MANIPULATION DARF NIE UNSERE DEMOKRATIE GEFÄHRDEN«

MARGARETE SCHRAMBÖCK,
BUNDESMINISTERIN FÜR DIGITALISIERUNG
UND WIRTSCHAFTSSTANDORT

INTERVIEW STEPHAN SCOPPETTA

Mittlerweile lassen sich über eine digitale Identität (E-ID) bereits viele Rechtsgeschäfte und Services auch der Republik Österreich nutzen. Wie wichtig ist die digitale E-ID in einer modernen vernetzten Gesellschaft?

Margarete Schramböck: Eindeutige Identitäten, wie über die ID Austria gegeben, sind in einer modernen vernetzten Gesellschaft der Grundpfeiler für die sichere Nutzung jeglicher digitalen Dienste. Besonders die Covid-Pandemie hat gezeigt, wie wichtig digitale Angebote als Ergänzung sind. Das Digitale Amt hatte während der Pandemie einen großen Zulauf.

Wie gut ist Österreich in diesem Bereich im internationalen Vergleich?

Im EU-Vergleich belegen wir Platz 3 im Bereich E-Government. Österreich nimmt seit Jahren mit der Handy-Signatur eine Vorreiterrolle ein. Ein Drittel aller Österreicherinnen und Österreicher ab dem 14. Lebensjahr besitzt eine Handy-Signatur. Über eIDAS können auch EU-Bürgerinnen und Bürger mit ihrer elektronischen Identität österreichische digitale Dienste nutzen. Im internationalen Vergleich ist Österreich einer jener Pioniere, die sehr stark auf die umfassende Nutzbarkeit der mobilen Devices setzen: „E-Government“ wird für uns immer mehr zu „M-Government“, also zum „Mobile Government“. Die meisten Nutzerinnen nutzen ihr Smartphone als primäres Device, um online zu gehen. Darum wollen wir hier auch bei den Serviceangeboten der Verwaltung sichere und einfach nutzbare Lösungen anbieten.

Welchen Ausbau wird die E-ID in den nächsten Jahren in Österreich erfahren?

Zurzeit wird an der Fertigstellung und Inbetriebnahme der ID Austria als Erweiterung der Handy-Signatur gearbeitet, mit dem auch zusätzliche Nachweise wie etwa Wohnsitz, Alter, Familienstand, aus zentralen Registern online erbracht werden können. Auch die Nutzung im EU-Ausland wird damit möglich werden. Ein weiterer wichtiger Ausbauschritt ist die Bereitstellung digitaler Aus- und Nachweise wie zum Beispiel des digitalen Führerscheins. Zusätzlich zu dem ständig wachsenden Angebot an E-Government-Diensten wird die ID Austria auch für die Wirtschaft angeboten. Somit können interessante digitale Dienstleistungen sicher angeboten werden.

Eine sichere digitale Identität braucht auch einen Rechtsrahmen. Wie weit ist dieser bereits in Österreich vorhanden?

Die notwendigen rechtlichen Grundlagen sind vorhanden. Österreich war der erste EU-Mitgliedstaat mit einem umfassenden





Margarete Schramböck, Bundesministerin für Digitalisierung und Wirtschaftsstandort, über die Möglichkeiten der neuen staatlichen digitalen Identität, Mobile Government und eine Teilnahme an Wahlen via Computer vom eigenen Wohnzimmer aus.

Rechtsrahmen für E-Government und einem eigenen E-Government-Gesetz. Dieses wird stetig weiterentwickelt, gemeinsam mit den notwendigen Adaptierungen weiterer Rechtsvorschriften.

Es gibt bereits die unterschiedlichsten Anbieter am Markt, die sich mit dem Thema digitale Identität beschäftigen. Wird es in Zukunft nur eine „staatliche“ digitale Identität geben (wie einen Reisepass) oder wird es verschiedene Anbieter geben, die entsprechend zertifiziert werden?

Mit der Identity Austria bietet der Staat ein sicheres und vertrauenswürdiges Instrument an, das umfassend genutzt werden kann. Durch die behördliche Identitätsprüfung, die

der Ausgabe zugrunde liegt, ist gewährleistet, dass tatsächlich diese bestimmte Person hinter der elektronischen Identität steht, die dies behauptet. Wir haben beim Ausstellungsprozess in Zukunft dieselbe Sicherheit wie bei der Ausstellung eines Reisepasses oder Personalausweises. Damit ist ein verlässlicher, rechtlich geregelter, staatlich verantworteter Identitätsnachweis auch in der elektronischen Welt möglich. Dieser kann für digitale Services der Verwaltung ebenso eingesetzt werden wie für Services in der Wirtschaft. Wenn ein Unternehmen andere Identitätslösungen akzeptiert, steht es diesem frei. Anderen Lösungen müssen sich aber in puncto Sicherheit, Verlässlichkeit und Datenschutz mit der Identity Austria-Lösung messen lassen. Identity Austria wird in Zukunft auch in den anderen EU-Staaten umfassend einsetzbar sein, weil der europäische Rechtsrahmen eine gegenseitige Anerkennung dieser staatlich gesicherten eID-Systeme vorsieht. Auch dies ist ein Vorteil gegenüber Alternativlösungen aus privater Hand.

Ist denkbar, dass wir schon bald unsere Stimme bei Gemeinderats-, Landtags oder auch Nationalratswahlen vom heimischen Computer abgeben?

Das könnte in Zukunft durchaus denkbar sein. Eine sehr einfache und gerne genutzte Möglichkeit zur demokratischen Partizipation gibt es über die digitale Unterstützung von Volksbegehren mit der Handy-Signatur und in Zukunft mit der ID Austria.

Muss uns das als Bürger nicht Angst machen und wird damit einer elektronischen Wahlmanipulation nicht Tür und Tor geöffnet?

Manipulation darf nie unsere Demokratie gefährden. Klar ist, dass elektronische Wahlen nur unter höchsten Sicherheitsstandards ablaufen können.

Kritiker einer E-ID warnen auch vor einer verstärkten staatlichen Kontrolle. In machen Diktaturen auf diesem Globus werden die digitalen Mittel zur Bürgerüberwachung bereits massiv genutzt. Wie kann ein Missbrauch der E-ID durch den Staat verhindert werden?

Datenschutz und Datensicherheit haben bei der Konzeption und Umsetzung höchste Priorität. Nicht nur deshalb, weil beide Bereiche die tragenden Säulen des Gesamtsystems bilden, sondern weil auch das Vertrauen der Nutzerinnen und Nutzer gewährleistet werden muss. ▀

»WIR SCHAFFEN EINE IDENTITÄT FÜR DIE WIRTSCHAFT UND DIE KONSUMENT:INNEN«

HARALD FLATSCHER, MANAGING DIRECTOR DER PSA PAYMENT SERVICES AUSTRIA GMBH, ÜBER DIE NOTWENDIGKEIT EINER DIGITALEN IDENTITÄT IM INTERNET, DEN UNTERSCHIED ZWISCHEN EINER PRIVATEN UND STAATLICHEN E-ID UND DIE NEUE ICH.APP.

INTERVIEW STEPHAN SCOPETTA

Warum ist eine eindeutige Identität im Internet notwendig?

Harald Flatscher: Im Grunde ist eine eindeutige digitale Identität nur eine Fortentwicklung des Bestehenden. Heute hat man bei jede:r Online-Händler:in oder anderen digitalen Serviceanbieter:innen im Internet einen Benutzernamen und ein Passwort. Gerade durch die Pandemie hat sich nun noch mehr Geschäft ins Internet verlagert und die Flut an Benutzernamen und Passwörtern hat für die Konsument:innen weiter zugenommen, was weder für die Anbieter:innen noch die Konsument:innen von Vorteil ist. Viel einfacher wäre es doch, einmal eine digitale Identität festzulegen und diese bei all meinen Online-Käufen und Services zu nutzen.

Welche Vorteile haben Konsument:innen und Konsumenten dadurch?

Mit einer digitalen Identität wie der neuen ich.app der PSA registrieren sich Nutzer:innen nur einmal und können sich mit dieser Identität bei allen Service-Partnern und Shops mit wenigen Klicks registrieren. Ein zentrales Thema dabei ist, dass für die Kund:innen maximaler Datenschutz gewährleistet ist. Der/die Kund:in weiß immer, wem er/sie welche Daten gibt.

Neben Ihnen als privatem Anbieter gibt es auch eine staatliche E-ID. Wo liegen hier die Unterschiede?

Nur der Staat kann in Österreich so etwas ausstellen wie einen digitalen Reisepass. Eine solche staatliche Identität ist erforderlich und nützlich beim Aufsetzen von digitalen Bürgerdiensten wie etwa dem Bezug von Strafregister-

auszügen oder Meldebestätigungen. Aber für den Einkauf im Internet braucht man keinen Reisepass, sondern zum Beispiel nur einen Identitätsnachweis etwa über eine Bank. Wichtig ist dabei, dass die Person eindeutig identifiziert ist.

Wo liegt hier nun der Unterschied zwischen einer staatlichen und einer privaten digitalen Identität?

Schafft der Staat mit ID Austria eine Identität für die/den Bürger:in, so schaffen wir als Finanzdienstleister eine Identität für die Wirtschaft und die Konsument:innen. Diese Teile ergänzen sich ideal und könnten gemeinsam zu einer ID für die Österreicher:innen werden. Daher sind wir mit den staatlichen Vertreter:innen in engem Austausch darüber, wie man beide Plattformen verknüpfen könnte.

Welche Vorteile ergeben sich aus einer Verknüpfung?

Durch eine Verknüpfung beider Welten könnte eine Identität geschaffen werden, mit der die Österreicher:innen einfach und sicher sowohl private als auch öffentliche Leistungen digital beziehen können. Das wäre wiederum ein idealer Beschleuniger um Österreich in der Digitalisierung aller Bereiche massiv voran zu bringen.

Wer letztendlich die meisten Akzeptanzpartner hat, wird das Match gewinnen?

Generell muss jedes neues System Nutzen stiften und im Falle einer digitalen Identität auch Relevanz erreichen. Das heißt, aus Sicht der Akzeptanzpartner wird wichtig sein, dass



möglichste jede/r Österreicher:in diese ID hat und nützt, aus Sicht der Konsument:innen wird es wichtig sein, dass sie eine digitale Identität möglichst überall verwenden können.

Welche neue Geschäftsfelder ergeben sich für Sie durch die Entwicklung der ich.app?

Wir sind der Überzeugung, dass wir mit der ich.app ein Problem lösen, ansonsten werden wir keinen Erfolg haben. Letztendlich ist sie ein wichtiges Tool für die Akzeptanzpartner, denn wir wissen, dass viele Online-Käufe im Grunde bei der Bezahlung abgebrochen werden. Können die Warenkörbe meist noch ohne Registrierung gefüllt werden, muss bei der Bezahlung ein Online-Formular ausgefüllt werden und das auch noch am Handy. Dabei vergeht vielen die Lust zum Einkauf oder sie verschieben diesen und vergessen dann darauf. Mit der ich.app ginge das mit wenigen Klicks, die Identität wäre hinterlegt und nur noch der Bezahlprozess muss abgewickelt werden.

Dieser ist also in der digitalen Identität nicht hinterlegt?

Das sehen wir als getrennte Prozesse. Die ich.app ist ein Identitätstool, aber kein Bezahl-Instrument. Aber natürlich ließe sich das auch auf Händlerseite verknüpfen und auch dafür werden wir in Zukunft Tools zur Verfügung stellen.

Drängen im Bereich E-ID nicht schon internationale Player auf den Markt?

Das Thema digitale Identität ist in Österreich derzeit sehr wenig besetzt und hier lässt

sich noch einiges bewegen. Zudem gibt es viele Use Cases, die noch nicht abgedeckt sind. Bei den internationalen Playern stellt sich zudem immer die Frage, wie der Datenschutz für die Nutzer:innen geregelt ist. Wir unterliegen auf jeden Fall strengen Regelungen in Österreich und die Kund:innen können sich sicher sein, dass wir wie eine Bank sehr sorgsam mit diesen Daten umgehen werden. Bei uns werden Daten auch nicht gespeichert, sondern wir vernetzen nur Daten, die/der User:in bei jedem Geschäftsfall freigibt.

Gehen Sie davon aus, dass es in Zukunft viele verschiedene Anbieter von digitalen Identitäten in Österreich geben wird?

Es werden noch Anbieter in diesem Feld auf den Markt drängen. Durchsetzen werden sich jene Lösungen, die den Kund:innen den meisten Mehrwert aufgrund der Usability und auch der Zahl der Akzeptanzpartner bieten werden. Dieses Rennen ist noch offen und wir haben sicher eine sehr gute Platzierung.

Wann startet die ich.app?

In den nächsten Wochen gehen wir in die Pilotphase über und danach kommt der letzte Feinschliff. Wir gehen davon aus, dass wir im Q2 des nächsten Jahres damit auf den Markt kommen werden. Wir wollen nach Markteintritt rasch die Grenze von einer halben Million Nutzer:innen schaffen und dafür brauchen wir natürlich Relevanz und damit viele Akzeptanzpartner:innen. An diesem Thema arbeiten wir aber schon sehr intensiv. ▀

Die PSA wickelt 1,2 Milliarden Transaktionen pro Jahr ab und betreibt 7.543 Bankomaten in Österreich. Die GmbH steht im Eigentum der heimischen Banken, größte Anteilseigner sind die Bank Austria, die Erste Bank und die BAWAG.

Flatscher ist seit März 2017 Geschäftsführer.

» BRAUCHEN MUT, UM DAS NEUE ANZUNEHMEN «

CHRISTOPH MAMMERLER, BUSINESS
DEVELOPMENT DIRECTOR DACH BEI CRIF

CRIF ist international einer der führenden Lösungsanbieter:innen
für Identitäts-Risikomanagement und Betrugsvermeidung.
Christoph Mammerler über Chancen und Risiken der digitalen Identität.

INTERVIEW OLIVER JANKO

Wie werden wir uns in fünf Jahren online ausweisen?

Christoph Mammerler: Wir bewegen uns zunehmend in einer digitalen Welt. Dementsprechend ist die digitale Identität essentiell. So wie wir in der realen Wirklichkeit die Person eindeutig identifizieren können – ein Ausweis und der Fotoabgleich mit der Person, die vor mir steht, reichen dazu –, gilt dieser Anspruch auch im Digitalen. Durch die rasche Digitalisierung, die durch die COVID-Pandemie eine Beschleunigung erfahren hat, hat die digitale Identifikation an Bedeutung gewonnen. Wir stehen zurzeit vor dem Vielfalts-Dilemma. Aus dem dringenden Bedarf sind viele verschiedene Identifikations-Methoden und -verfahren entstanden. Einige davon, die einen physischen Abgleich digital abbilden oder mittels Video-Chat, Ausweiserkennung und mittels Handykamera die „echte“ Person verifizieren. Aus diesen sogenannten phygitalen Identifikations-Verfahren haben wir uns in eine digitale Identifizierbarkeit hin entwickelt. Doch auch hier ist noch eine erstmalige Feststellung der Identität in physischer Form notwendig – also dann, wenn die digitale Identität an die physische Person ausgegeben wird.

Die Vision der Zukunft muss sein, dass, egal in welchen Welten wir uns bewegen, die Identität der Person eindeutig, sicher und einfach feststellbar ist. Einfach darum, da es die Online-Konsument:innen gewöhnt sind, sich frei und userfreundlich in der Online-Welt zu bewegen. Dass sie für diese Usability oftmals einen hohen Preis zahlen – über Single-Sign-on mit meinem Social-Media-Account registriert und mein Userverhalten kennen mehr Leute als mir lieb ist – diese Awareness ist in der Bevölkerung noch nicht da. Das wird aber zunehmend ein Thema und darum braucht es sichere, transparente und vor allem datensparsame Wege. Auch mehr Selbstbestimmtheit und Datenhoheit bei jeder/m Einzelnen.

Die Verifizierung online ist vor allem im E-Commerce-Bereich relevant. Wer aber verwaltet künftig meine persönlichen Daten? Wie sieht das digitale Amt aus und wie wird dort meine Sicherheit garantiert?

Die Entwicklung der Vielfalt von Identifikations-Möglichkeiten ist nicht mehr aufzuhalten. Und das ist gut so, denn nur so findet Entwicklung und technologische Evolution statt. Durch die Digitalisierung und ihren technologischen Möglichkeiten brechen Konventionen auf. Wie beispielsweise Online-Banken, die das traditionelle Bild des Bankings revolutionieren, was einen Paradigmenwechsel im Banking Sektor zur Folge hat.

Das digitale Amt wird nicht die große Revolution auslösen. Vielmehr wird es ein weiterer möglicher Weg sein. Als CRIF-Gruppe

unterstützen wir die Macht der Vielfalt und setzen mit unserem ganzheitlichen Identifikations-Ansatz einen neuen Maßstab.

Das heißt, als Endergebnis könnten wir wieder verschiedene Lösungen verwenden müssen, richtig?

Ich sehe das mehr als eine Chance, die wir uns zu Nutze machen sollen. Dabei sind Simplifizierung, Transparenz, Usability und Demokratisierung die erfolgsentscheidenden Attribute der Digitalisierung. Der Drang nach Neuem und Innovation prägt die Digital Generation. Wir brauchen Agilität und Mut das Neue anzunehmen und mitzugestalten.

Was macht es so schwierig, eine Lösung für staatliche und privatwirtschaftliche IDs zu finden?

Die Schwierigkeit ist die Qual der Auswahl. Die digitale Identität eindeutig festzustellen bringt im Online-Business nicht nur mehr Sicherheit gegen Onlinebetrug, vielmehr bedingen manche Geschäftsprozesse die rechtskonforme Identifizierung, wenn es sich beispielsweise um den Abschluss einer Online-Versicherung oder eines Handyvertrags handelt, wie auch bei der Eröffnung eines Online-Bankkontos.

Es gibt nicht die eine Methode, die für alle Konsument:innen die eine richtige ist. Dafür sind bereits zu viele unterschiedliche Verfahren im Umlauf und je nach Sicherheitsstufe mehr oder weniger sinnvoll bzw. notwendig. Und wie auch bei den Zahlungsmethoden geht es um die Usability, sprich den Konsument:innen ist es wichtig, selbst wählen zu können, mit welcher Methode sie sich identifizieren möchte. Zudem gibt es laufend neue Methoden der Identifikation und auch in seiner technologischen Umsetzung stets Entwicklung. Hier kann man als Händler:in gar nicht den Überblick behalten.

Wie könnten mögliche Lösungen aussehen?

Wir geben der Vielfalt eine „Bühne“ und vereinen die verschiedensten Identifikations-Möglichkeiten auf einer Plattform. Dieser PaaS-Ansatz macht es den Unternehmen – sprich den Händler:innen und den Konsument:innen – maximal einfach und convenient: Als Identification Service Provider bietet CRIF über die Plattform die Vielzahl von Identifikations-Methoden an, die je nach Anforderung entlang der Customer Journey maßgeschneidert eingesetzt werden. Somit bietet der/die Onlinehändler:in die notwendige Auswahl und hat mit uns den Überblick über die Must-Haves der Identifikations-Branche. Und das über Landesgrenzen hinweg, im deutschsprachigen Raum und auch in Europa. ▀



»Die Vision der Zukunft muss sein, dass egal in welchen Welten wir uns bewegen, die Identität der Person eindeutig, sicher und einfach feststellbar ist.«

CHRISTOPH MAMMERLER
Business Development
Director DACH CRIF

In seiner Funktion ist Mammerler verantwortlich für den Lösungsvertrieb und die Entwicklung neuer digitaler Geschäftsfelder im internationalen Kontext.



DIGITALE IDENTITÄT IST LÄNGST REALITÄT

LUKAS PRAML, GESCHÄFTSFÜHRER DER STAATSDRUCKEREI IM GESPRÄCH

Die private Österreichische Staatsdruckerei bündelt in der younix Identity AG ihre Entwicklungen für eine sichere digitale Identität – wie das digitale Ausweissystem „My Identity App“ (MIA).

Die younix Identity AG wurde 2017 als Tochter-Startup der Staatsdruckerei Holding AG gegründet. Was waren damals die Ziele?

Wir haben Digitalisierung und digitale Identitäten immer als Chance gesehen. Als Österreichische Staatsdruckerei haben wir Identitäten schon seit Jahrhunderten geschützt. Unser Arbeitsmaterial besteht aber nicht mehr nur aus Papier, sondern genauso auch aus Bits und Bytes. Deshalb haben wir bereits 2012 einen eigenen Innovations-Bereich in der Staatsdruckerei gegründet mit dem Ziel, bei digitaler Identität selbst Akzente zu setzen. 2017 hat die Staatsdruckerei schließlich mit der younix Identity AG ein hauseigenes Digital-Startup ins Leben gerufen. Mit

den erfolgreichen Launches unserer inhouse entwickelten elektronischen Identität „MIA“ haben wir unser Ziel von 2012 umgesetzt und setzen heute Akzente im Bereich von digitalen Identitäten.

Der Software-Sektor gilt als sehr schnelllebig. Ein Rückblick vier Jahre später: Wie haben sich die Anforderungen an die digitale Identität in den letzten Jahren verändert?

Das gesamte Umfeld hat sich massiv verändert. Digitale Identität ist keine graue Theorie mehr. Weltweit haben Staaten mit der Digitalisierung von Behördenservices begonnen. Was vorher nur persönlich am Schalter möglich war, geht plötzlich komplett digital. Aber egal ob digital oder persön-

lich: Der sichere Nachweis meiner eigenen Identität ist immer der Eckpfeiler für alle Schritte.

Das haben Staaten in den letzten Jahren erkannt, allerdings gibt es teilweise deutliche Unterschiede bei der Umsetzung. Aktuell werden unterschiedliche Zugänge, verschiedene Konzepte und neue Technologien diskutiert. Ein Beispiel: Wie sollen die Bürgerinnen und Bürger ihre digitale Identität erhalten? Nur per persönlichem Besuch in der Behörde oder ist ein KI-unterstütztes Onboarding über das Internet möglich, etwa per Video-Ident-Verfahren? Ein großer Diskussionspunkt ist auch die Frage nach einer zentralen gegenüber einer dezentralen Lösung. Für mich persönlich ist vor allem die Fachdebatte zu SSL, also Self Sovereign Identity, derzeit eine der wichtigsten Weichenstellungen für die kommenden Jahre.

Bereits 2015 wurde mit der Entwicklung von MIA gestartet - der „My Identity App“. Mittlerweile arbeiten fast 30 Entwickler:innen von younix an der Anwendung. Wie funktioniert MIA - und wofür kann sie verwendet werden?

Wir haben mit MIA die weltweit erste vollintegrierte digitale Identitätslösung umgesetzt. MIA kombiniert digitale Ausweise und eine sichere eID-Funktion in einer einzelnen Smartphone-App. MIA deckt in einer

App also gleich zwei Bereiche von digitalen Identitäten ab und ist in Kooperation mit unseren Partner:innen in zwei europäischen Ländern bereits im Echtbetrieb im Einsatz. Zum Beispiel können viele Services der Liechtensteiner Behörden mit der auf MIA basierenden App „eID.li“ komplett digital genutzt werden. Im Kosovo ist MIA als digitaler Führerschein im Einsatz. Bei einer Verkehrskontrolle zeigt man dort den Führerschein am eigenen Smartphone vor.

Wie wird die Sicherheit gewährleistet?

Wir haben bei MIA von Anfang an auf „security-by-design“ gesetzt. Die Sicherheit persönlicher Daten wurde also von Beginn an mitgedacht. MIA authentifiziert sich über das Backend via Zertifikate, die sicher am Smartphone der Nutzer:innen gespeichert werden. Jeder Datentransfer von MIA ist über TLS (Transport Layer Security) gesichert. Der Vorteil: Es werden keine Daten am eigenen Smartphone dauerhaft gespeichert. Wenn das eigene Gerät verloren oder gestohlen wird, gibt es keinen Verlust von persönlichen Daten. Darüber hinaus werden zu keinem Zeitpunkt Daten zwischen dem persönlichen und einem prüfenden Gerät übermittelt, sondern alle Daten immer aus einer vertrauenswürdigen Quelle wie zum Beispiel dem Führerscheinregister abgerufen. Uns ist wichtig, dass die User:innen dabei die volle Kontrolle über den Prozess haben. Wenn ein digitaler Ausweis vorgezeigt wird, muss der/die User:inn explizit dem gesamten Prozess zustimmen, bevor Daten auf dem überprüfenden Gerät angezeigt werden. Damit hier sichere Rahmenbedingungen geschaffen werden, beteiligen wir uns international an der Ausarbeitung des entsprechenden ISO 18013-5 Standards für digitale Führerscheine.

Liechtenstein setzt schon seit 2019 auf die Technologie von younix. Wie ist die Zusammenarbeit zustande gekommen? Wofür wird MIA in Liechtenstein verwendet?

Nutzer:innen von „eID.li“ können schon seit Ende April 2020 bequem und sicher mit ihrem Smartphone oder per Computer die Services der Liechtensteinischen Behörden nutzen. Nach mehr als einem Jahr können wir ein positives Zwischenfazit ziehen. Rund die Hälfte aller Liechtensteiner:innen haben ihre persönliche eID.li aktiviert und nutzen die Services der Behörden auf digitalem



»Mit einer verifizierten digitalen Identität kann man sich sicher und bequem weltweit anmelden.«

LUKAS PRAML
Geschäftsführer Österreichische Staatsdruckerei GmbH & Vorstand younix Identity AG

Weg. Wir haben gemeinsam mit unserem Partner CRYPTAS International GmbH den Zuschlag für eine Liechtensteinische eID erhalten. Entwickelt wurde „eID.li“ dann hausintern in der younix Identity. Das Team unseres Partners CRYPTAS war für die Entwicklung der zentralen eID-Integrationsplattform verantwortlich.

Gibt es schon Pläne für weitere Länder?

Ja, wir verfolgen weltweit Ausschreibungen zu digitalen Lösungen

genau und nehmen entweder selbst oder gemeinsam mit unseren Partner:innen teil, zum Beispiel in Europa oder Nordamerika.

Zum Abschluss etwas allgemeiner: Wie werden wir uns in fünf Jahren im Internet ausweisen? Und wo steht younix in fünf Jahren?

Digitale Identitäten werden das Zentrum unseres Alltags sein. Sie sind ja schon heute nicht mehr aus dem öffentlichen Sektor wegzudenken. Man muss diese Entwicklung nur weiterdenken und sich fragen, bei wie vielen elektronischen Diensten man sich täglich anmeldet. Jede Authentifizierung mit Nutzernamen und Passwort lässt sich genauso durch eine digitale Identität auf Knopfdruck durchführen. Natürlich will man das nicht überall, Stichwort Anonymität. Aber meine Bank, ein Onlineversandhaus oder meine Versicherung müssen sehr wohl wissen, wer ich bin. Mit einer verifizierten digitalen Identität kann man sich sicher und bequem weltweit anmelden. Ich bin fest überzeugt, dass das in fünf Jahren der Standard sein wird. Und ich bin überzeugt, dass younix dafür die sicheren und vertrauenswürdigen Lösungen liefert. ▀



- ist die weltweit erste vollintegrierte digitale Identitätslösung, die digitale Ausweise und elektronische Identität in einer Smartphone-App vereint
- gibt dem/der User:inn volle Transparenz, welche persönlichen Informationen mit wem geteilt werden
- folgt einem User-zentrierten Design um die Nutzung so einfach wie möglich zu gestalten
- bietet Multi-Faktor-Authentifizierung via Biometrie (FIDO)
- ist ISO 18013-15 ready (online & offline)
- speichert persönliche Daten nie dauerhaft auf dem eigenen Gerät und beugt so Datenverlust bei Diebstahl oder Geräteverlust vor
- setzte von Anfang an auf „security-by-design“

MIA ist bereits in zwei europäischen Ländern im Echtbetrieb im Einsatz:

- im Fürstentum Liechtenstein ist MIA als digitale Identität „eID.li“ im April 2020 gestartet und bietet einfachen und komplett digitalen Zugriff auf viele Behördenservices
- In der Republik Kosovo ist MIA als „RKSmobileID“ seit Februar 2018 als digitaler Führerschein im Echtbetrieb verfügbar. Bei einer Verkehrskontrolle kann der eigene Führerschein komplett digital vorgezeigt werden.



TECHNOLOGIE

BLOCKCHAIN & SILO

DIE TECHNOLOGISCHE
SEITE DER IDENTITÄT



Aus Sicht der Nutzerinnen

und Nutzer ist schnell klar, wie ein virtueller Ort für wichtige personenbezogene Daten und Ausweise funktionieren soll: Er soll stets erreichbar und einfach zu bedienen sein, dabei maximal sicher und im Optimalfall noch umfangreich kompatibel. Das wissen auch die verschiedenen Unternehmen, die an Lösungen in diesem Bereich arbeiten. Funktioniert die Technologie hinter den Verifizierungsdiensten nicht immer perfekt oder gibt es Zweifel an ihrer Sicherheit, strafen die Nutzer:innen das sofort ab. Soll heißen: Sie wechseln den Dienst oder misstrauen dem Ganzen ohnehin.

Im Kern gibt es zwei Ansätze: Das Team rund um die ID Austria etwa setzt auf eine zentrale Lösung, das ist bei staatlichen Diensten oft auch unumgänglich. Nur der Staat verwaltet etwa Führerscheindaten - da ist es nur sinnvoll, auch die digitale Verteilung zentral zu steuern. Am freien Markt wiederum passiert so gut wie alles dezentral. Die Blockchain lässt grüßen: Was vor nicht allzu vielen Jahren noch maximal

Krypto-Insider:innen ein Begriff war, hat sich mittlerweile zu einer in vielen Bereichen gängigen Form der Datenorganisation gemausert. Es braucht hier keine zentrale vertrauenswürdige Instanz, die die Hoheit über die Daten hat, Datenbanken werden über die Blockchain auf viele Teilnehmer:innen und Knotenpunkte verteilt.

Wir wollten darum etwa von E-Commerce-Anbieter:innen wissen, wie ihre Lösungen aussehen und haben mit Expert:innen die unterschiedlichen Zugänge diskutiert. Letztlich stellt sich die Frage, welcher technologische Ansatz sich durchsetzen wird oder ob es, wie derzeit von vielen Expert:innen vermutet, verschiedene Lösungen mit unterschiedlichen Ansätzen werden. Und was wäre, wenn der Staat überhaupt nur als verifizierende Instanz eine Rolle spielt - und letztlich die Nutzer:innen wählen, welche Datensätze mit welchen Anbieter:innen verwaltet werden? 



SICHERHEIT UND FUNKTIONALITÄT: SO FUNKTIONIERT DIE DIGITALE IDENTITÄT



Hinter der digitalen Identität stecken Technologien, die Sicherheit und Funktionalität garantieren. Doch wie funktionieren Wallets, Blockchain, SSI und Co? Und was kommt da noch alles in der Zukunft?

TEXT ALOIS PUMHÖSEL

Aus Nutzersicht ist klar, wie ein virtueller Ort für wichtige personenbezogene Daten und Ausweise funktionieren soll – am besten allorts zugänglich und einfach bedienbar. Nur so kann eine hohe Akzeptanz in der Bevölkerung erreicht werden. Die IT-Dienstleister und staatlichen Instanzen hinter den virtuellen Ausweisen müssen lernen, diese Bürgernähe mit einem breiten Funktionsumfang und hoher Sicherheit in Einklang zu bringen. Wie sehen also jene Technologien aus, die hinter einer sicheren und niederschweligen digitalen Identität stehen? Und welche künftigen Weiterentwicklungsmöglichkeiten sind absehbar?

Vom Passwort zur Kryptografie

Beginnen wir mit einem Blick in die Vergangenheit: Während eine Passwort-Identifizierung für den Zugang zu Inhalten und Services das Internet seit seinen Anfängen begleitet, war die Entwicklung einer Reihe spezieller Technologien notwendig, um einen effektiven und für breite Nutzerschichten zugänglichen Identitätsschutz im Netz zu gewährleisten. Dazu zählt heute eine hoch entwickelte Kryptografie, leistungsfähige Cloud-Technologie oder automatisierte Kommunikation zwischen verschiedenen digitalen Systemen. Zudem sind Smartphones hilfreich, die ihren Benutzer:innen – mittlerweile über biometrische, auf Fingerabdruck oder Gesichtszügen basierende Sicherheitstechniken – eindeutig zugeordnet werden können.

Der Aufstieg der Blockchain

Gleichzeitig gewann im vergangenen Jahrzehnt auch eine radikal neue Form der Datenorganisation an Boden – dezentrale Systeme á la Blockchain. Die als Distributed-Ledger-Technologien zusammengefassten Ansätze benötigen keine zentrale vertrauenswürdige Instanz, die die Hoheit über die Daten hat, sondern verteilen die Datenbanken über viele Teilnehmer und Knotenpunkte. Die Technologie hat in vielen Bereichen einen festen Platz gefunden, etwa in ►

»Die Grundidentität muss noch immer vom Staat kommen. Er muss seine Register öffnen und bei einem dezentralen Konzept mitmachen.«

► der Organisation von Lieferketten oder bei Kryptowährungen. Die Internetwährung Bitcoin ist bis heute das bekannteste Blockchain-basierte Phänomen. Derartige verteilte Systeme werden auch in der Zukunft der digitalen Identitäten eine Rolle spielen. Wie groß ihre Bedeutung in diesem Bereich aber letztendlich sein wird, darüber sind sich Expertinnen und Experten allerdings noch uneinig.

Ein Experte, der in der Entwicklung der neuen digitalen Identität in Österreich, der ID Austria, eine große Rolle spielt, ist Arne Tauber. Der Wissenschaftler am Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz ist Generalsekretär des Zentrum für sichere Informationstechnologie Austria (A-SIT) und leitet das E-Government Innovationszentrum (EGIZ), das in die Konzeption und Umsetzung der ID Austria maßgeblich involviert ist. Tauber betont: „ID Austria baut auf einem Identitätsmanagement auf, bei dem zentrale Systeme eine wesentliche Rolle spielen. Hier gibt es zentral organisierte Komponenten, denen man absolut vertrauen kann.“ Damit ist Österreichs keineswegs allein: Ein Großteil aller digitalen Identitäten aus dem staatlichen und privaten Bereich weltweit setzt auf konventionelle, zentrale Architekturen. Dezentrale Systeme werden in bestimmten Szenarien künftig dennoch eine wesentliche Rolle spielen. Im Moment wird auf EU-Ebene an den rechtlichen Grundlagen dafür gearbeitet.

Drei Komponenten für die ID Austria

Drei grundsätzliche Komponenten organisieren im zentralen System der ID Austria die digitale Identität, erläutert der IT-Security-Experte. Da sind zum einen die Verwaltungsregister, in denen die personenbezogenen Informationen abgelegt sind – etwa das Personenstandsregister oder das zentrale Melderegister. Zum anderen gibt es Vertrauensdiensteanbieter, die für die Authentifizierung zuständig sind und sicherstellen, dass die sich anmeldende Person tatsächlich jene ist, die sie vorgibt zu sein. ID Austria setzt dabei auf eine qualifizierte elekt-

ronische Signatur. Als dritte Komponente agiert zwischen diesen Systemen ein sogenannter Identity-Provider als Schnittstelle in Richtung der Nutzerapplikation. „Er leitet Anfragen an den Vertrauensdiensteanbieter zu Benutzerauthentifizierung weiter, kommuniziert mit den Komponenten zur Bereitstellung der Identitätsattribute, garantiert, dass diese Daten nur mit Zustimmung der Benutzer weitergegeben werden und übermittelt die Identitätsdaten der anfragenden Applikation retour“, zählt Tauber auf.

Dealbreaker Authentifizierung

Gerade die Authentifizierung ist ein wesentliches und kritisches Element des Gesamtsystems. „Eine Herausforderung ist dabei bei entsprechend hoher Sicherheit ebenfalls eine hohe Benutzerfreundlichkeit zu garantieren“, sagt Tauber. Trotz mehrstufiger Maßnahmen darf die Anmeldung nicht zu umständlich werden. Die ID Austria setzt hier wie die Handy-Signatur als technischer Vorgänger auf eine bewährte Mehrfaktorauthentifizierung mit Passwort und dem Nachweis des Besitzes eines Mobilgeräts.

„In vielen anderen Ländern sind eigene Signaturkarten, die über einen Chip verfügen, Standard. Diese Lösung hat im Vergleich zur österreichischen Variante allerdings das Problem, dass man aufgrund der Technologie zu wenige Benutzer:innen erreicht. Denn dafür sind eigene Softwareinstallationen und Kartenleser notwendig und die Lösungen funktionieren nur auf bestimmten Geräten“, erklärt Tauber. In absehbarer Zukunft soll hier mit der Kompatibilität der ID Austria mit FIDO (Fast Identity Online) eine weitere Möglichkeit zur Authentifizierung geschaffen werden, betont der Forscher. Nutzer:innen benötigen dabei nicht mehr unbedingt ein Handy für die Authentifizierung, sondern können neben dem Signaturpasswort auch den sogenannten FIDO Token nutzen.

Führerschein am Handy

Eine künftige Weiterentwicklung, die auch bei der ID Austria ansteht, ist eine Ausweisplattform, bei der Führerschein, Zulassungsschein und andere Dokumente in digitaler Form bereitgestellt und damit

NETWORK SECURITY

beispielsweise am Handy präsentiert werden können. Damit würde nun auch ein dezentrales Element dazukommen, betont Tauber. Die Ausweisdaten liegen dabei aus Datenschutzgründen in digitalen „Brieftaschen“, sogenannten Wallets, üblicherweise am Mobilgerät selbst. Beim Vorzeigen der Ausweise erfolgt die Kommunikation direkt zwischen dem Ausweisbesitzer und dem Prüfer, kein zentrales System ist somit in den Vorgang involviert. Das beugt auch Überwachungsängsten vor. „Niemand kann nachvollziehen, wenn jemand in einem Nachtclub war und dort einen Altersnachweis vorweisen musste“, veranschaulicht Tauber. „Mittels welcher Technologie dieser Ansatz in Österreich umgesetzt wird, ist noch offen. Distributed-Ledger-Technologien sind hier nur eine von mehreren Möglichkeiten.“

Datensouveränität

Der Ansatz der Ausweis-Wallets übernimmt bereits Aspekte einer sogenannten Self Sovereign Identity, also einer digitalen Identität, bei der die Hoheit über die Daten nicht bei einer zentralen, vom Staat verwalteten Instanz liegt, sondern bei jedem einzelnen Bürger – ein Bereich, in dem intensive Forschungen laufen. Tauber arbeitet etwa in EU-Forschungsprojekten an Konzepten der Self Sovereign Identity mit. Ein Ziel ist etwa, dass die Datenbrieftasche hier auch sicher in der Cloud verschlüsselt abgelegt werden kann – ohne dass der Cloud-Anbieter darauf zugreifen könnte. Grenzüberschreitende ID-Systeme werden ermöglicht und die Basis für einen Datenmarkt geschaffen, in dem Nutzer selbst entscheiden, welche Daten sie Dienstleistern oder der Wissenschaft zur Verfügung stellen wollen. Die eigenen Daten können dabei durch die Benutzer selbst vermarktet werden – und nicht nur wie bisher durch große Internetkonzerne.

Vom Passwort zur Kryptografie

Eine Self Sovereign Identity in einer noch viel stärkeren Ausprägung gilt vielen Initiativen aus Wirtschaft und Zivilgesellschaft als eine zukunftsweisende Lösung. Hier geht man davon aus, dass die gesamte digitale Identität dezentral organisiert sein sollte. „Unsere digitalen Identitäten gehören nicht uns. Sie gehören jenen Organisationen, die uns die Identität geben. Heute sind das nicht nur Staaten, sondern vor allem auch private Konzerne wie Facebook oder Google, die so unsere Nutzerdaten verwerten können“, erklärt Alfred Taudes, der sich am Forschungsinstitut für Kryptoökonomie der Wirtschaftsuniversität Wien und der Forschungseinrichtung Austrian Blockchain

Center mit den Möglichkeiten der verteilten Systeme beschäftigt. Er ist ein Fürsprecher einer weitgehenden Self-Sovereign-Identität auf Basis von Blockchains. Damit sei die Möglichkeit gegeben, diese Datenhoheit von den Digitalkonzernen zurückzugewinnen.

„Der Staat würde in einem derartigen System die Rolle einer verifizierenden Instanz spielen. Wenn ich also angebe, Österreicher zu sein, würde der Staat diese Angabe im Abgleich mit dem Melderegister bestätigen“, veranschaulicht Taudes. „Meine Identität als Österreicher würde dann also als sogenanntes Verified credential in meiner digitalen Brieftasche verwaltet. Der virtuelle Amtsstempel kann auch leicht wieder eingezogen werden, wenn die entsprechenden Voraussetzungen nicht mehr gegeben sind – etwa wenn ein Führerschein abläuft oder sich eine Meldeadresse ändert.“

Identität für das Auto

Auch Datenmärkte seien damit einfach umsetzbar. Banken könnten beispielsweise die Daten, die sie ohnehin über Kund:innen sammeln, verwerten, indem sie – natürlich mit Autorisierung des Kunden/der Kundin – die Bonität bei einem Autokauf bestätigen. Genauso könnten Unternehmen ihre Datenbanken ohne viel Pflegeaufwand aktuell halten. Das Blockchain-System ist für Taudes aber letzten Endes auch eine Voraussetzung für eine künftige Machine Economy, in der also technische Systeme über eigene digitale Identitäten interagieren und Transaktionen durchführen. Taudes gibt ein Beispiel: „Sowohl ein Elektroauto als auch eine Wallbox zum Stromtanken haben dann eine digitale Identität, die in einer Blockchain abgelegt ist. Wenn man nun bei einer fremden Wallbox lädt, kann der Vorgang automatisch – etwa über Kryptowährung – abgerechnet werden.“

In einer ganzen Reihe von Ländern gibt es bereits Unternehmenskonsortien, die eine Self Sovereign Identity promoten – beispielsweise IDUnion in Deutschland. Österreich habe schon allein wegen des zentralen Melderegisters gute Voraussetzungen für ein System dieser Art, glaubt der Kryptoökonomie-Forscher. Die Frage ist, ob sich der Staat mit der lediglich verifizierenden Rolle zufrieden gibt. Taudes: „Die Grundidentität muss noch immer vom Staat kommen. Er muss seine Register öffnen und bei einem dezentralen Konzept mitmachen.“



ALFRED TAUDES
Professor an der
WU Wien, Krypto-
ökonomieforscher



ARNE TAUBER
Generalsekretär des
Zentrum für sichere
Informations-
technologie Austria



» ES MUSS EIN POLITISCHER WILLE ENTSTEHEN «

GERHARD KRAMMER FÜR DEN VEREIN FÜR DIGITALES VERTRAUEN

INTERVIEW OLIVER JANKO

Neben der staatlichen Lösung ID Austria und diversen unternehmerischen Ansätzen gibt es „MeineSichereID“, hinter dem der „Verein für digitales Vertrauen“ steht. Wie sieht Ihr Ansatz aus?

Gerhard Krammer: Wir beschäftigen uns seit 2018 mit dem Thema „Digitale Identität“, oder besser mit dem Austausch von identitätsbezogenen Daten. Das Ziel ist, den Dokumentenordner, den jeder zu Hause im Regal stehen hat, zu digitalisieren und in der digitalen Welt nutzbar zu machen.

Für dieses Daten-Ecosystem gelten für uns ein paar Grundsätze. Erstens: dezentral statt zentrale Silos. Daten sollen immer dezentral im Wallet der Nutzerin gespeichert werden. Es gibt keine Möglichkeit Daten an einer Stelle einzusehen, bzw. dass diese damit gesamt in falsche Hände geraten. Zweitens: Standard statt proprietär. SSI hat sich als kommunikativer Standard herauskristallisiert und wird schrittweise im W3C standardisiert. Und drittens: gemeinnützig statt gewinnorientiert. Um so ein Ecosystem zu betreiben, braucht es entsprechende Governance und damit eine Dachorganisation. Diese muss gemeinnützig sein und bestmöglich vor einer Übernahme geschützt werden.

Vor der Pandemie mussten wir die Sinnhaftigkeit identitätsbezogener Daten noch mühsam erklären. Seit letztem Jahr fragen alle nur noch, warum wir das nicht schon längst umgesetzt haben. Corona hat unser Leben verändert. Von Online-Shopping bis Home Office hat sich der Bedarf an Identitätsattributen enorm gesteigert und ist in allen Bereichen unseres Lebens angekommen.

Beim Ansatz von „MeineSichereID“ soll „der Mensch als Souverän seiner digitalen Identität“ im Mittelpunkt stehen. Können Sie das genauer erläutern?

Das ist ein wesentlicher Punkt in der Architektur der Plattform. Heute weiß niemand mehr, welche seiner/ihrer persönlichen Daten wo gespeichert sind und was genau damit gemacht wird. In dem SSI-Netzwerk gibt es drei Rollen. Den Issuer oder Aussteller, den Verifier oder Verwender und den Owner oder Eigentümer der Daten. Ein Aussteller stellt einen Datensatz zur Verfügung und signiert diesen. Zum Beispiel ein Uni-Abschlusszeugnis, signiert von der WU Wien. Dieser Datensatz wird im Wallet der Eigentümerin abgespeichert. Ein Verwender, z.B. ein Headhunter, benötigt nun diesen Datensatz und fordert ihn von der Eigentümerin an. Diese muss die Übermittlung am Handy freigeben, damit ihr Uni-Zeugnis zum Headhunter kommt und dort automatisch verarbeitet wird. Die einzige, die eine Weiterleitung ihrer Daten veranlassen kann, ist immer die Person, um deren Datensatz es sich handelt. Damit sind wir auch völlig DSGVO-konform. Der Datensatz kann von der Eigentümerin auch jederzeit zurückgezogen, aktualisiert oder mit einer zeitlichen Gültigkeit ausgestellt werden. Der Aussteller hat keine Information darüber, wo sein signierter Datensatz verwendet wird. Das ist wie in der analogen Welt. Die Universität hat auch keine Infos darüber, wo ihr Zeugnis verwendet oder hergezeigt wird. Bei zentralen Systemen weiß immer jemand über alle Aktivitäten Bescheid und dokumentiert diese.

»Vor der Pandemie mussten wir die Sinnhaftigkeit und Notwendigkeit identitätsbezogener Daten noch mühsam erklären. Seit letztem Jahr fragen alle nur noch, warum wir das nicht schon längst haben.«

Wer unterstützt den Verein?

Aktuell haben wir 14 aktive Mitglieder. Die Österreichische Staatsdruckerei mit ihrer Tochter Younix, die Notartreuhandbank, die RLB NÖW, A1 und Drei, die Post, die Raiffeisen Informatik, die APA als Vertreterin der Medien, ekey, der Handelsverband, die gemdat NÖ und OSSBIG. Kürzlich dazu gestoßen sind der Compass-Verlag und die A-Trust als österreichischer Vertrauensdiensteanbieter.

Darüber hinaus gibt es noch Unterstützer:innen und Berater:innen, wie beispielsweise Prof. Taudes von der WU Wien bzw. Austrian Blockchain Center oder Thomas Lohninger von epicenter.works. Unser Ansatz und die Bandbreite der Unternehmen stoßen auf großes Interesse. Neue Mitglieder sind immer willkommen.

Vereine sind gemeinnützig orientiert. Ein Vorteil oder Nachteil in diesem Bereich? Das Projekt muss schließlich auch finanziert werden.

Gemeinnützigkeit ist meiner Meinung nach wichtig, damit ein derartiges Ökosystem funktioniert. Sobald Gewinnorientierung dahinter steht, dauert es nicht lange und wir diskutieren nur noch über Shareholder Value.

Was wir hier aufbauen, ist eine notwendige Infrastruktur für digitales Business. Wir sind quasi die ASFINAG und bauen unsere Straßen, damit wir nachher darauf fahren können. Unser Ziel ist, dass auf dieser Infrastruktur neues digitales Geschäft entsteht. Von der Digitalisierung von Prozessen, über neue Produkte und Services, bis zu Geschäftsmodellen, die heute noch gar nicht möglich sind.

Die Finanzierung ist tatsächlich ein Problem. Unternehmen zu motivieren, in eine allgemein nutzbare Infrastruktur zu investieren, ist sehr schwierig. In anderen EU-Ländern, wo der politische Wille stärker ausgeprägt ist, klappt die Finanzierung gemeinsam mit dem Staat.

In Österreich gibt es einige Unternehmen und Konsortien, die versuchen, eine ID-Lösung zu etablieren. Der Staat setzt auf ID Austria. In Deutschland beispielsweise gibt es vier große Projekte, bei denen der Staat und die Privatwirtschaft beteiligt sind. Warum klappt das bei uns nicht?

In Deutschland unterstützt die Bundesregierung tatsächlich ähnliche privatwirtschaftliche Konsortien mit über 60 Millionen Euro für die kommenden drei Jahre. Das ist aber kein Geschenk, sondern ein PPP-Modell. Die rund 70 Unternehmen in vier Konsortien investieren die gleiche Summe noch einmal.

Deutschland hat früh erkannt, dass ein solches System nur gemeinsam mit der Wirtschaft und anderen Organisationen funktionieren kann. Das entspricht im Wesentlichen auch der Aufforderung der EU-Kommission an die Mitgliedstaaten, Konzepte mit der Wirtschaft zu entwickeln. Denken Sie an mein Beispiel mit dem Uni-Abschlusszeugnis. ID vom Staat, Zeugnis von der Uni und der/die

Bürger:in verwendet das mit einer privatwirtschaftlichen Headhunter:in. Ich bin fest davon überzeugt, dass nur eine Zusammenarbeit erfolgreich sein kann. Die Systeme stehen in keinem Konkurrenzverhältnis, sondern müssen sich optimal, für die Menschen, ergänzen. Unsere Türe steht dafür offen.

Würden Sie sich also mehr Zusammenarbeit, mehr Kooperation zwischen den einzelnen Partner:innen wünschen?

Wir sprechen mit allen Partner:innen, die derartige Systeme entwickeln. Eine Zusammenarbeit ist immer vorstellbar, solange unsere Grundprinzipien, wie dezentrale Speicherung, keine Gewinnorientierung und das Aufsetzen auf Standards nicht beeinträchtigt werden. Eine Zusammenarbeit mit einem zentralen Datensilo würde die Grundidee von SSI komplett konterkarieren. Man kann aber Daten daraus nutzen und diese im Wallet des/der User:in speichern.

Wir tauschen uns regelmäßig mit Partner:innen aus, die SSI-Systeme planen oder bereits aufbauen. Anfang Oktober gibt es wieder einen großen Videocall von Finnland über die Niederlande, Deutschland, Schweiz, bis Italien und Spanien. Hier ist auch die Interoperabilität immer ein großes Thema.

Sie sehen „MeineSichereID“ als „Ergänzung für die Wirtschaft“ und keine Konkurrenz zur ID Austria. Einfach gefragt: Wie soll diese Ergänzung aussehen?

Neben den staatlichen Attributen gibt es eine Vielzahl von Attributen der Wirtschaft und anderen Organisationen, die absolut notwendig sind, um ein digitales Business zu entwickeln. Ich habe mit unzähligen Unternehmen gesprochen, um deren Bedarf abzuholen. Da geht es um personalisierte Tickets und den legalen Weiterverkauf, um Einkommensnachweise für Kredite, Loyalty-Programme im Handel oder einfach um die ÖAMTC-Pannenhilfe um nur ein paar Beispiele zu nennen. Die Palette ist unvorstellbar groß und ich bin davon überzeugt, dass wir erst an der Oberfläche kratzen. Eine einheitliche Login-Lösung ist ohnehin eine Basisfunktionalität und kann hunderte Passwörter ablösen. Wir sprechen derzeit von Personen und Unternehmen. Der gesamte IoT-Bereich ist hier noch gar nicht berücksichtigt.

Wie groß sehen Sie die Chance, dass sich auch hierzulande noch alle Beteiligten „zusammenraufen“?

Ich bin immer optimistisch. Denken Sie an das Beispiel mit dem Uni-Zeugnis. Staat, Universität, der/die Bürger:in und der der/die Headhunter:in. So kann das alles zusammenspielen.

Ich denke, dass wenn der Nutzen von den Stakeholdern erkannt wird und ein entsprechender politischer Wille entsteht, dann werden wir gemeinsam ein solches Projekt erfolgreich umzusetzen. Wir sind bereit und ich freue mich persönlich darauf. ▀

»Die Gemeinnützigkeit ist, meiner Meinung nach, ein wesentliches Fundament, damit ein derartiges Ecosystem funktioniert. Sobald Gewinnorientierung dahintersteht, dauert es nicht lange und wir diskutieren nur noch über Shareholder Value und ähnliche Dinge.«



GERHARD KRAMMER ist Senior Partner der BUSINESS DESIGN, einer Agentur für Geschäfts- und Organisationsentwicklung in Wien. Sie entwickelt seit über 10 Jahren neue Produkte und Services, schlagkräftige Geschäftsmodelle und leistungsfähige Organisationen. In dieser Rolle leitet er das Projekt „MeineSichereID“ und steuert die Aktivitäten des Vereins für digitales Vertrauen.

VIER FÜR EIN STARKES DIGITALES EUROPA PRINZIPIEN

Die "Open Source Software Business Innovation Group" ist ein Verein, der sich die "Stärkung des Wirtschaftsstandorts Österreich und Erhöhung der regionalen IT-Wertschöpfung" auf die Fahne geheftet hat. Open Source-Software soll in Wirtschaft und Politik verbreitet werden. Damit will OSSBIG die digitale Selbstbestimmung erhöhen. Der Verein hat dafür vier Prinzipien verabschiedet. International ist OSSBIG Mitglied des GAIA-X-Projekts für eine souveräne, europäische Dateninfrastruktur und Mitglied im „Verein für digitales Vertrauen“. In diesem Kontext beschäftigt sich OSSBIG auch mit der digitalen Identität.

Digitalisierung und die „data driven economy“ bestimmen unseren künftigen Wohlstand. Sie verändern Wertschöpfungsketten und die Spielregeln der Märkte. Digitalisierung ist getrieben durch Daten, Vernetzung und Algorithmen, ermöglicht durch Maschinenpower und Orchestratoren - also digitale Plattformen.

Die zunehmende Digitalisierung von Geschäftsprozessen hat einen globalen, de facto nach den Regeln der „Big Player“ agierenden Wirtschaftsraum entstehen lassen. In der digitalen, international vernetzten Welt waren darum bisher nur wenige, sehr große, global agierende Unternehmen erfolgreich. Diese wenigen Unternehmen speichern heute auch den größten Teil der weltweiten Daten, den Rohstoff für digitale Geschäftsmodelle und das Training künstlicher Intelligenzen. Die Menge an Daten wird mit zunehmender Nutzung digitaler Angebote und steigendem Reifegrad neuer Technologien weiter zunehmen.

Europa hinkt nach

Informationstechnologie ist nicht mehr nur Werkzeug zur Optimierung und Automatisierung, sondern Basis für die Umsetzung von politischen und wirtschaftlichen Strategien.

Europa spielt in der digitalen Welt allerdings eine untergeordnete Rolle. Keines der neu entstandenen, globalen Internet-Unternehmen stammt aus Europa. Die Abhängigkeit vor allem von US-amerikanischen IT-Anbietern und chinesischer Produktion hat sich zunehmend vergrößert. Was bisher ein zu verkraftender Wettbewerbsnachteil war, wird mit zunehmender strategischer Bedeutung der Digitalisierung zu einer erheblichen Bedrohung für die Selbstbestimmung von Bürger:innen, Staat und Wirtschaft.

Herausforderungen für Europa

Die aktuelle Herausforderung für Europa und Österreich besteht deshalb darin, Handlungsfähigkeit von Bürger:innen, Staaten und Unternehmen zu erhalten und den Handlungsspielraum zu erweitern. Handlungsfähigkeit setzt voraus, Optionen zu kennen, sie zu sehen, diese zu bewerten und zu verstehen, aus den Optionen zu wählen und diese umsetzen zu können. ▮

KONTAKT:
info@ossbig.at



OPENNESS

VERBREITUNG VON OPEN SOURCE,
OPEN DATA, OPEN STANDARDS,
OPEN INNOVATION



EMPOWER- MENT

ERHÖHUNG LOKALER, DIGITALER
KOMPETENZ UND DER ANZAHL
DIGITALER EXPERT:INNEN



COLLA- BORATION

FÖRDERUNG DER ZUSAMMEN-
ARBEIT PRIVATER UND
ÖFFENTLICHER ANWENDER:INNEN
IN DEN BEREICHEN INNOVATION
UND DIGITALISIERUNG



TRUST- WORTHINESS

VERTRAUEN IN DATEN UND IHRE
HERKUNFT, IN TECHNOLOGIEN UND
ORGANISATIONEN





DER KAMPF GEGEN ONLINEBETRUG

Der Onlinehandel wächst unaufhaltsam und mit ihm auch der Onlinebetrug. Betroffen sind jedoch nicht nur Unternehmen, sondern auch Kund:innen, die mit dem Diebstahl ihrer Identität konfrontiert sind. Es gilt deshalb mehr Aufmerksamkeit für die Gefahr des Onlinebetruges zu schaffen, um präventiv agieren zu können.

INTERVIEWS HELENE TUMA

GERALD SEBASTIAN EDER

HEAD OF BUSINESS DEVELOPMENT
E-COMMERCE, CRIF AUSTRIA

Herr Eder, mit der Beliebtheit des Online-Handels steigt für die Händler:innen auch das Risiko, Opfer von professionellem Betrug zu werden.

Gerald Sebastian Eder: CRIF führt jährlich eine DACH-weite Studie zum Thema Onlinebetrug durch. Die Ergebnisse zeigen auch 2021, dass neun von zehn Onlinehändler:innen bereits Opfer von Betrug/Betrugsversuchen geworden sind. Und obwohl die Zahl bereits in den letzten Jahren sehr hoch war, sehen auch heuer noch über 40 Prozent der Befragten diese Gefahr als steigende. Da stellt sich die Frage, ob in Zukunft alle von Onlinebetrug betroffen sein werden. Wir sehen diesen Trend leider auch durch unseren täglichen Austausch mit unseren E-Commerce-Kund:innen bestätigt. Und die Betrüger:innen werden immer professioneller und sind technologisch bestens ausgestattet.

Wie gehen die Betrüger:innen vor?

Jeder Onlinebetrug hat in irgendeiner Weise

immer mit Identität zu tun. Zu den häufigsten Betrugsformen zählen dabei laut unserer Studie die „verfälschte Identität“, also die Angabe falscher Namens- und/oder Adressdaten mit 76 Prozent und mit 75 Prozent hoch im Kurs ist es auch die Identität zu „stehlen“, sprich die Identität eines anderen für den Raubzug zu verwenden. In Österreich ist es zudem mit fast 70 Prozent „beliebt“, eine völlig erfundene Identität zum Onlineshopping zu verwenden. Man kann letztendlich jeden Onlinebetrug auf die Identität zurückführen. Eine sichere digitale Identität – das ist meiner Meinung nach wichtigste Thema im Kampf gegen Onlinebetrug.

Wie schwierig ist es für Unternehmen das richtige Maß zwischen größtmöglicher Sicherheit und Alltagstauglichkeit zu finden?

Die Balance zwischen Sicherheit und trotzdem für die Kund:innen eine angenehme Customer Journey zu bieten und sie bei Shoppinglaune zu halten, ist die größte Herausforderung. Es gilt das Gesetz der Usability: Werden die Kund:innen in seiner/ihrer Shoppinglaune durch ein kompliziertes Identitätsverfahren gestört, besteht Abbruchgefahr. Hier punkten jene Onlineshops mit mehreren Identifikationsmöglichkeiten, aus denen die Kund:innen selbst wählen. //



RAINER WILL

GESCHÄFTSFÜHRER HANDELS-
VERBAND ÖSTERREICH

Herr Will, welche Vorkehrungen können Unternehmen treffen, um sich selbst vor Betrugsversuchen und Ihre Kund:innen vor Identitätsmissbrauch zu schützen?

Rainer Will: Kriminelle agieren hochprofessionell. Ebenso professionell müssen wir bei der Abwehr von Betrugsversuchen vorzugehen. Um verdächtige Verhaltensmuster bereits proaktiv zu erkennen, empfehlen wir datenbasierte Technologien sowie den Einsatz moderner Betrugsvermeidungs-Tools. Erfreulicherweise setzen mittlerweile bereits 80 Prozent der heimischen Webshops konkrete Maßnahmen zur Fraud Prevention ein. Um das Betrugsrisiko zu reduzieren, kombinieren sie meist verschiedenste Schutzmaßnahmen – und verzichten dafür auch auf potenzielle Mehrumsätze.

Wo geht der Weg Ihrer Meinung nach in Zukunft hin?

Das größte Zukunftspotenzial sehen wir in der „digitalen Identität“. Warum? Jeden

Tag identifizieren wir uns digital – sei es beim Lesen von Online-Medien, beim Posten in den sozialen Netzwerken oder beim Bezahlen im Webshop. Nachweispflichten sind bereits allgegenwärtig, sowohl im privatwirtschaftlichen als auch im öffentlichen Sektor. Gleichzeitig stellen fehlende digitale Nachweise eines der größten Digitalisierungshemmnisse unserer Zeit dar. Jetzt geht es darum, Strukturen zu schaffen, die zum einen eine nutzerfreundliche Ausstellung und Übermittlung digitaler Nachweise gewährleisten, zum anderen aber auch alle relevanten Bereiche wie Technologie, Recht, Sicherheit, Wirtschaftlichkeit und Datenschutz berücksichtigen.

Braucht es eine europäische Lösung?

Als Handelsverband unterstützen wir schon seit Jahren verschiedenste Self Sovereign Identity-Initiativen (SSI) zum Aufbau eines europäischen Ökosystems für digitale Identitäten. Im Kern geht es darum, dass alle Bürger:innen ihre persönlichen Daten und Nachweise selbstbestimmt verwalten und kontextbezogen teilen können. Wir wollen damit einen „Datenschutz made in Europe“ entwickeln, von dem sowohl die Endverbraucher:innen als auch die Wirtschaft profitieren. ▀



FLORIAN FLOCK

SENIOR CONSULTANT NICESHOPS

Herr Flock, welche Vorkehrungen haben sie bei niceshops getroffen, um Ihr Unternehmen vor Betrugsversuchen und Ihre Kund:innen vor Identitätsmissbrauch zu schützen?

Florian Flock: Für uns als Onlinehändler:innen ist besonders der Bestellbetrug eine unangenehme Situation und wir versuchen diese Versuche stark einzudämmen. Ein von uns selbst entwickeltes System versucht betrügerische Bestellungen zu erkennen, sie werden daraufhin händisch kontrolliert. Für ein geschultes Auge stechen diese Bestellungen meist hervor, da sie immer ähnliche Muster aufweisen. Bei Kreditkartenzahlungen nutzen wir eine der modernsten Erkennungsmechanismen zur Betrugserkennung. Es kombiniert Signale aus Userverhalten, Bestelldaten, historischer Transaktionen usw. und erstellt einen Risk-Score. Damit haben wir den Kreditkartenbetrug mehr oder weniger den Riegel vorgeschoben.



Würden Ihre Kund:innen auch strengere Onboarding-Prozesse mittragen?

Ich denke, dass unsere Kund:innen es sehr schätzen, wenn wir strengere Maßnahmen im Einsatz haben – es geht immerhin um den Schutz jeder Einzelnen. Vieles läuft ohnehin im Hintergrund ab, beispielsweise die Echtzeit-Überprüfung von Bestellungen direkt im Check-out. Davon bekommen Kund:innen in der Regel nichts mit. Aber meine persönliche Einschätzung ist, dass strengere Maßnahmen positiv wahrgenommen werden. Jedoch ist viel Kommunikationsarbeit und Aufklärung notwendig.

Sind Sie mit den bisher angebotenen Lösungen zufrieden? Würden sie bestimmte Dinge noch brauchen?

Wir sind in der glücklichen Lage und können auf hochqualifizierte Kolleg:innen in der IT zurückgreifen. Dahingehend wurden einige Komponenten selbst entwickelt, so wie wir uns Betrugserkennung vorstellen und wie es auch praktikabel ist. Das funktioniert sehr gut für uns und skaliert auch mit. Abgerundet werden die Eigenentwicklungen dann noch mit diversen Fremdsystemen im Paymentbereich. Insgesamt ergibt das für uns ein schlüssiges Konzept zur Betrugserkennung. ▀

WIR HABEN IHRE DATEN!

RANSOMWARE-ANGRIFFE WERDEN EIN GRÖßERES PROBLEM. BARRACUDA HILFT.

Ransomware-Angriffe auf die Privatwirtschaft sind an der Tagesordnung und immer mehr nehmen Kriminelle verstärkt öffentliche Institutionen ins Visier. Erst kürzlich hat das Nationale Zentrum für Cybersicherheit (NCSC), vor möglichen Fällen im Gesundheitswesen gewarnt. Nichts und niemand ist gefeit vor Lösegeld-Forderungen mittels krimineller Datenverschlüsselung - egal ob KMU oder Konzern. Wichtig also: Sicherheitsvorkehrungen.

Cyberkriminelle verwenden bösartige Software, die als E-Mail-Anhang oder Link bereitgestellt wird, um das IT-Netzwerk zu infizieren und E-Mails, Daten und andere wichtige Dateien zu sperren, bis ein Lösegeld - vorzugsweise in einer Kryptowährung - gezahlt wird. Diese sich ständig weiterentwickelnden und immer raffinierteren Angriffe sind schädlich und sehr kostspielig. Hohe finanzielle Verluste aufgrund von Ausfallzeiten, Lösegeldzahlungen, Wiederherstellungskosten und anderen nicht budgetierten und unvorhergesehenen Ausgaben sind die Folgen. Wichtig ist also, dass vielfältig vorgesorgt wird.

Lösegeld und Datenverletzung

Nicht nur Angriffe sind aber auf dem Vormarsch. Auch Lösegelder und Lösegeldzahlungen steigen. In vielen Fällen werden Lösegelder nun häufiger

gezahlt, und diese Forderungen gehen in die Millionen Euro. Cyberkriminelle stehlen nicht nur Daten und verschlüsseln Dateien mit anschließender Lösegeld-Forderung, sondern verlangen auch Zahlungen von den Opfern, um zu vermeiden, dass die gestohlenen Informationen öffentlich werden, was gegebenenfalls zu einer massiven Rufschädigung des Unternehmens führen könnte. Viele Cyberkriminelle kombinieren inzwischen den Einsatz von Ransomware und Datenverletzungen, um auf diese Weise den erpresserischen Druck auf ihre Opfer zu erhöhen. Wird der Lösegeldforderung nicht nachgegeben, legen die kriminellen die gestohlenen Daten auf eigene Server ab oder versteigern diese im Dark Web.

Verteidigung gegen Ransomware-Angriffe

Die sich schnell entwickelnde Bedrohungslage erfordert fortschrittliche



DR. KLAUS GHERI
General Manager
Network Security,
Barracuda Networks

Gheri, Vorstandsvorsitzender der Barracuda Networks AG, leitet mit der Firewall-Sparte einen der wichtigsten Unternehmensbereiche des Security-Spezialisten aus den USA.

BARRACUDA

Die Barracuda Networks AG, die nach wie vor Österreich als wichtigen Standort hat, ist aus einem Startup hervorgegangen. Gheri gründete im Jahr 2000, mitten im Dotcom-Hype, mit Phion eine Jungfirma, die sich schnell im Security-Bereich einen Namen machte. 2009 übernahm die Barracuda-Gruppe Phion mehrheitlich.

Advanced Firewalls

Wenn ein Benutzer einen bösartigen Anhang öffnet oder auf einen Link zu einem Drive-by-Download klickt, bietet eine fortschrittliche Netzwerk-Firewall, die Malware-Analysen durchführen kann, eine Chance, den Angriff zu stoppen, indem sie die ausführbare Datei beim Versuch, sie zu passieren, kennzeichnet.

Erkennung von Malware

Bei E-Mails mit bösartigen Dokumenten im Anhang kann sowohl die statische als auch die dynamische Analyse Hinweise darauf liefern, dass das Dokument versucht, eine ausführbare Datei herunterzuladen und auszuführen. Die URL für die ausführbare Datei lässt sich oft mithilfe von Heuristiken oder Threat Intelligence-Systemen erkennen. Eine durch statische Analyse erkannte Verschleierung kann ebenfalls darauf hinweisen, dass ein Dokument verdächtig sein könnte.

Sperrlisten

Da der IP-Speicherplatz immer begrenzter wird, verwenden Spammer zunehmend ihre eigene Infrastruktur. Oft werden dieselben IPs lange genug verwendet, damit eine Software sie erkennen und zu einer Blacklist hinzufügen kann. Selbst bei gehackten Websites und Botnets ist es möglich, Angriffe vorübergehend nach IP zu blockieren, sobald ein ausreichend großes Spam-Volumen erkannt wurde.

Schulung des Benutzerbewusstseins

Phishing-Simulationen sollten Bestandteil von Sicherheitsschulungen sein, um zu gewährleisten, dass Endanwender Angriffe erkennen und vermeiden können.

Backup

Im Falle eines Ransomware-Angriffs kann eine Cloud-Backup-Lösung Ausfallzeiten minimieren, Datenverluste verhindern und Systeme schnell wiederherstellen, ganz gleich, ob sich die Dateien auf physischen Geräten, in virtuellen Umgebungen oder in der Public Cloud befinden. Idealerweise sollte die 3-2-1-Regel mit drei Kopien aller Dateien auf zwei verschiedenen Medientypen befolgen, von denen mindestens eine ausgelagert ist. So wird vermieden, dass Backups von einem Ransomware-Angriff bedroht werden. ▀

ein- und ausgehende Sicherheitstechnologien, die über das herkömmliche Gateway hinausgehen. Dazu gehört auch das Schließen der technischen Lücken und die Schulung der Mitarbeiter für größtmögliche Sicherheit bei geringstem Risiko, Opfer von ausgeklügelten Ransomware-Angriffen zu werden.

Spam-Filter/Phishing-Erkennung

Auch wenn viele bösartige E-Mails überzeugend wirken, können Spam-Filter, Phishing-Erkennungssysteme und ähnliche Sicherheitssoftware subtile Hinweise identifizieren und dazu beitragen, dass potenziell bedrohliche Nachrichten und Anhänge erst gar nicht in den E-Mail-Posteingang gelangen.

Ein erfolgreicher Ransomware-Angriff kann den Unternehmensbetrieb schlagartig zum Erliegen bringen. Um Business Continuity zu gewährleisten, wenn wichtige Dateien nicht mehr verfügbar sind, ist ein aktuelles Backup der Daten zur zügigen Wiederherstellung unabdingbar.

Egal ob als sicheres Anmelde-
detool im E-Commerce-Bereich,
als digitales Amt oder als Wallet
für Führerschein und Co: Die eID
- oder digitale Identität - wird Kon-
sument:innen und Konsumenten in
den nächsten Jahren (hoffentlich)
das Leben erleichtern.

Während staatliche Lösungen
vorrangig dafür gedacht sind, die
Behörden des Landes in den digi-
talen Raum zu transferieren, ver-
suchen Unternehmen und Vereine,
Lösungen für privatwirtschaftliche
und persönliche Zugänge und Do-
kumente zu etablieren. Doch was
bedeutet das für die einzelne Kon-
sumentin, den einzelnen Konsu-
menten? Im oberösterreichischen
Kremsmünster etwa läuft bereits
ein Pilotprojekt mit der ID Aust-
ria, mit der Behördenservices, das
Postamt und eben der Ausweis
noch digitaler werden sollen. Die
ID ersetzt dabei im ersten Schritt
die ungeliebte Handysignatur.

Wichtig dabei aus Konsumenten-
sicht: Optimaler Schutz ist bei der
digitalen Transformation ein abso-
luter Schlüsselaspekt, schließlich
verwaltet die Wallet - egal ob von
staatlicher oder privatwirtschaft-
licher Seite - eine Menge persö-
nlicher und damit oft auch heikler
Daten.

Jurist Viktor Mayer-Schönberger
spricht in diesem Zusammenhang
auch von mehreren Identitäten,
die wir künftig wohl verwalten und
schützen werden müssen.

Die Sicherheit der persönlichen
Daten wird allerdings nicht in allen
Staaten dieser Welt derart intensiv
diskutiert. China gilt als Land der
"gläsernen Bevölkerung", die Kom-
munistische Partei belohnt "gutes"
und straft "schlechtes" Verhalten.

Geheimnisse vor den Behörden
gibt es kaum noch. Nur: Steht der
Westen wirklich besser da? "Wir
gucken nach China und denken,
wir stehen im Trockenen. Aber
europäische Werte alleine helfen
nicht gegen Überwachung. Es
braucht auch politische Hand-
lungen", sagt etwa die Sinologin
und Politikwissenschaftlerin Ka-
tika Kühnreich. Vielerorts tapen
Konsument:innen dahingehend
aber noch im Dunklen, die meisten
ID-Lösungen harren noch in den
Startlöchern. Klar ist nur: Das Aus-
weisen im digitalen Raum wird sich
nach und nach verändern. ▀

A photograph of a crowd of people at an outdoor event. In the foreground, a hand holds a smartphone, capturing a photo or video. The background shows several people, including a man with sunglasses and a woman with long, wavy hair. The scene is brightly lit, suggesting a sunny day.

**WER HAT
.. DIE MACHT
ÜBER DIE
EIGENEN
DATEN?**

DIGITALE IDENTITÄT UND DER STAAT

IN KREMSMÜNSTER LÄUFT DER ID AUSTRIA-PILOTVERSUCH

TEXT GERRIT GUBO

Großes Potenzial, ausbaufähige Reglementierung: Etliche Staaten scheitern trotz steter Bemühungen an der Etablierung flächendeckend genutzter digitaler Identitäten, obwohl „Personalausweise“ in der Online-Welt immer stärker an Relevanz gewinnen. Eine Studie des Consulting-Giganten McKinsey ergab, dass die Häufigkeit der Verwendung der digitalen Identität in den meisten Staaten mit etablierten Systemen pro Person im Durchschnitt nicht über zweimal im Jahr liegt. Dabei birgt die digitale Identität hohes Potenzial – Online-Sicherheit und Vermeidung von Internet-Betrug sind nur zwei der großen Assets, die eine regulierte Online-Identifikation mit sich bringen würde.

Der digitale Alltag

Im vergangenen Jahrzehnt wurde das Online-Leben ebenso real wie die analoge Welt. Social Media, Online-Shopping, Bankgeschäfte – Konsumenten treten im Netz auf wie im „echten Leben“, doch viele dieser Interaktionen verlangen nach einer geprüften Identität. Problematisch wird es, wenn viele dieser Identitäten vorhanden sind – was durch verschiedene Nutzerkonten bei unterschiedlichen Online-Portalen der Fall ist – denn hier kommen auch Management der Login- ▶



id:0110101010101

id:01010101000001



Die Bezirkshauptmannschaft Kirchdorf ist als Pilot-BH für die digitale Identität der ID Austria ausgewählt worden. Bürgerinnen und Bürger können mit Herbst 2021 umsteigen.



»Verbraucher legen verstärkt Wert auf die Absicherung ihrer digitalen Daten.«

MAG. DANIELA ZIMMER,
Expertin für Konsumentenpolitik

► Daten und Passwörter ins Spiel. Aus Konsument:innen-Perspektive wäre eine geprüfte digitale Identität hier von Vorteil, da langwierige Anmeldevorgänge und zig verschiedene Passwörter damit der Vergangenheit angehören würden. Was eine solche digitale Identität zumindest beinhalten müsste, weiß Mag. Reinhard Haider, Amtsleiter der Marktgemeinde Kremsmünster: „Eine digitale Identität muss zumindest europatauglich sein und muss so wie der Reisepass absolut verlässlich die Identität nachweisen, also mit Namen, Geburtsdatum und der Ausstellung der qualifizierten Signatur.“ Aber die Forderung nach einer offiziellen digitalen Identität wirft auch komplexe Fragestellungen auf, denen man nur schwer habhaft wird. So steht man zualererst vor dem Problem der Ausstellungsgenehmigung: Wie bei allen offiziellen Dokumenten muss auch ein digitaler Ausweis behördlich genehmigt werden. Oder? Fakt ist, dass der digitale Raum weitaus weniger Reglementierungen unterliegt als die physische Welt, somit ist auch (noch) nicht festgehalten, ob es ein staatliches Monopol auf die Ausstellung digitaler Identitäten geben wird.

»Die Hoheit über das Ausstellen digitaler Identitäten muss der Staat haben, denn es handelt sich um die digitale Infrastruktur der Zukunft«, zeigt sich Reinhard Haider überzeugt.

Staat oder Privatanbieter?

Die Europäische Kommission schlug Anfang Juni einen Rahmen für eine europaweite digitale Identität vor. Mit der EUid soll Bürger:innen und Unternehmen ein Identitätsnachweis zur digitalen Weitergabe von Dokumenten sowie der Nutzung europaweiter Online-Dienste dienen. Ein weiterer geplanter Schritt ist die Ausstellung einer digitalen Brieftasche, in der der Identitätsnachweis mit amtlichen Dokumenten verknüpft wird – wie dem Bankkonto, dem Führerschein und Zeugnissen. Auch einzelne Staaten haben sich bereits weiter auf das Terrain vorgewagt und Pilotprojekte gestartet: In Österreich nimmt die Gemeinde Kremsmünster die Vorreiterrolle in puncto digitaler Identität ein. Seit Juli läuft das Projekt der ID Austria, einem elektronischen Identitätsnachweis, der sich als weiterentwickelter Hybrid aus Handysignatur und Bürgerkarte präsentiert, hier im Echtbetrieb. „Die E-Signatur hat vor wenigen Jahren den Höhenflug begonnen, als die App des Bundes »Digitales Amt« das Ummelden von Wohnsitzen, das Unterschreiben von Volksbegehren oder das Einholen von Strafreisgerbescheinigung binnen drei Minuten möglich machte. Die ID Austria soll jetzt auch die Legitimation der Bürger vor den Behörden ermöglichen und mit der digitalen Unterschrift damit papierlose bzw. medienbruchfreie Prozesse möglich werden. Denken wir nur an das Senden oder auch das persönliche Aushändigen von Unterlagen“, so Haider.

E-Postkasten, digitale Amtsservices, Wirtschaftsgeschäfte – das soll nur der Anfang der Möglichkeiten des digitalen Ausweises

sein. Auch die von McKinsey durchgeführte Studie sieht die digitale Interaktion zwischen Individuum und Staat betreffend bis dato schlummerndes Potenzial, denn neben der Beschleunigung von Amtsprozessen, einer daraus resultierenden Kostenreduktion und der Minderung des Risikos von Identitätsbetrug wären digitale Wahlen eine sich eröffnende Option. Für Staaten ergibt sich daraus natürlich ein weiterer Anreiz, flächendeckende digitale Identitätsnachweise zu forcieren, da höhere Wahlbeteiligung und Bürgerpartizipation auf diese Funktion digitaler Identitäten folgen könnten. Nach wie vor bleibt allerdings die Frage nach der Beschaffung jener digitalen Identität offen: Wer ist berechtigt, diese auszustellen, und welche Kriterien müssen Anbieter erfüllen, falls nicht nur staatlich verfasste Identitäten anerkannt werden? Die Vorteile im Falle von privaten Anbietern liegen für Konsument:innen auf der Hand: Auf Basis von Angebot und Nachfrage gelte das Prinzip des freien Marktes, verschiedene Anbieter böten unterschiedliche Services, Optionen und Preise. Andererseits ergäbe sich daraus erneut ein Problem: Welche Unternehmen respektive Handels- und Geschäftspartner, ganz zu schweigen von staatlichen Services, erkennen von welchem Anbieter ausgestellte Identitäten an? Reinhard Haider vertritt eine klare Ansicht: „Wer, wenn nicht der Staat, sollte für eine unveränderbare Identität bürgen? Privatanbieter können und sollen auf der ID Austria aufsetzen und passende Applikationen entwickeln.“ Außerdem: „Wenn der Staat für die (digitale) Identität zuständig bleibt, dann bürgt er auch dafür. Dass die demokratischen Staaten und die Beamten das können, beweisen sie schon jahrzehntelang und das darf sich auch bei der Transformation in ein digitaleres Leben nicht ändern.“

Datenschutz

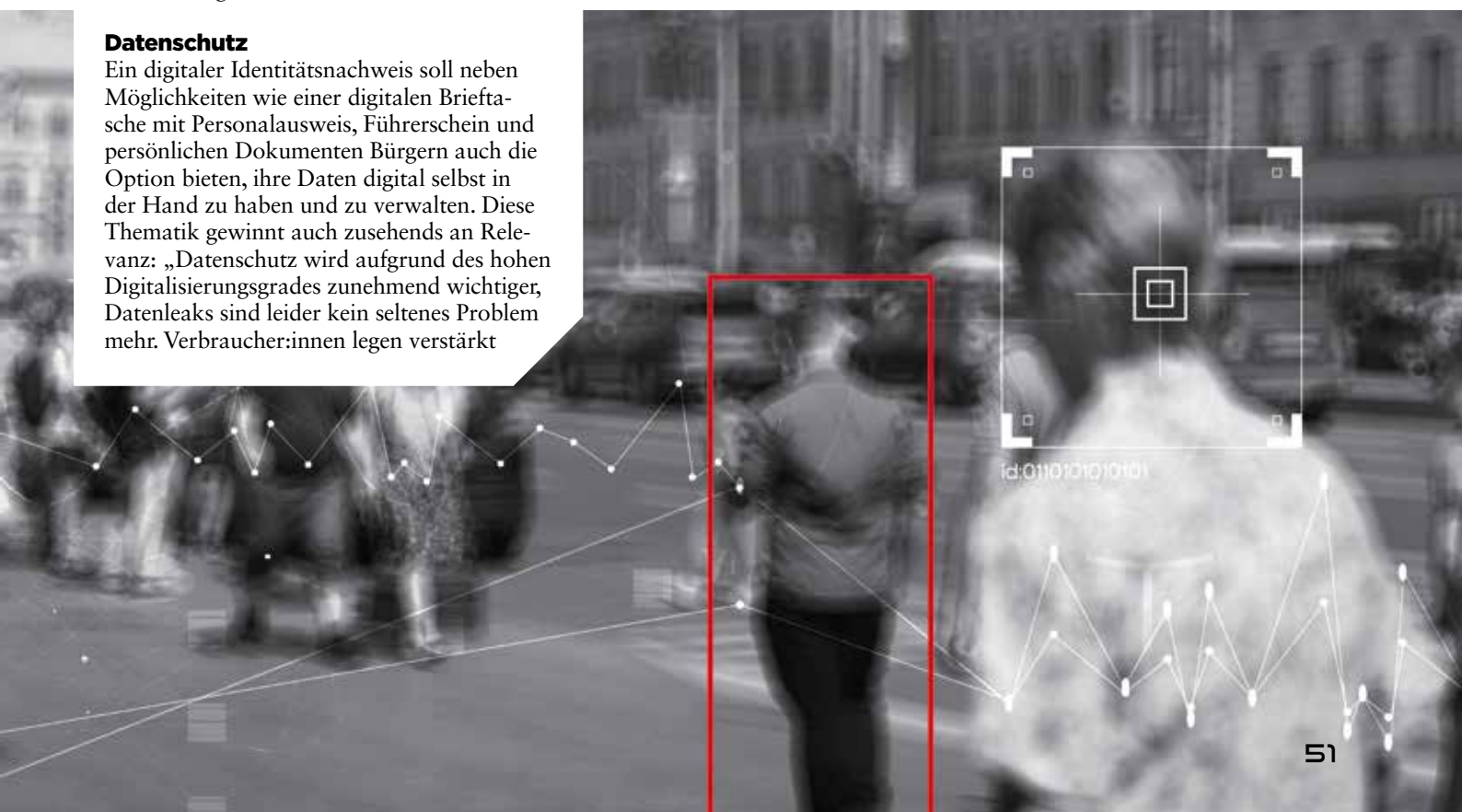
Ein digitaler Identitätsnachweis soll neben Möglichkeiten wie einer digitalen Brieftasche mit Personalausweis, Führerschein und persönlichen Dokumenten Bürgern auch die Option bieten, ihre Daten digital selbst in der Hand zu haben und zu verwalten. Diese Thematik gewinnt auch zusehends an Relevanz: „Datenschutz wird aufgrund des hohen Digitalisierungsgrades zunehmend wichtiger, Datenleaks sind leider kein seltenes Problem mehr. Verbraucher:innen legen verstärkt

Wert auf die Absicherung ihrer digitalen Daten“, erklärt Daniela Zimmer, Expertin für Konsumentenpolitik bei der Arbeiterkammer Wien. Da drängt sich die Frage auf, ob persönliche Daten durch offizielle digitale Identitäten überhaupt geschützt wären: Die gesammelten Daten einer Person, alle vereint in einem digitalen Identitätsnachweis, können zurecht als hochsensibles Material gehandelt werden. „Dem Konsumentenschutz muss wichtig sein, dass nicht zu viele Daten gespeichert werden und diese Daten im Sinne der Datensicherheit vom Bund unter Verschluss gehalten werden“, sagt Haider. Gesellen sich neben Führerschein, Reisepass, Zeugnissen und anderen offiziellen Dokumenten auch biometrische Daten wie Fingerprint und Gesichtserkennung hinzu, werden Datenleaks und Hackerangriffe zur Katastrophe. Dass Gesichtserkennung und Fingerprint anstelle von Passwörtern nicht zwangsläufig ratsam sind, findet auch Daniela Zimmer: „Besonders bei biometrischen Daten sind die Folgen der Entwendung fatal – das Passwort kann man ändern, die eigene Fingerkuppe oder das Gesicht nicht. Wir empfehlen daher, bei Alltagsgeschäften ein Passwort anstelle biometrischer Daten zur Identifikation zu verwenden.“ Ob mit- oder ohne biometrische Daten: dass die digitale Identität ein Teil der Zukunft ist, steht jedenfalls fest – dass sie den digitalen Alltag verbessern wird, davon ist Reinhard Haider überzeugt: „Im Sinne des Konsument:innen sollte auch der Konsumentenschutz offen sein für die vielen Möglichkeiten, die eine digitale ID bieten kann.“



»Wer, wenn nicht der Staat, sollte für eine unveränderbare Identität bürgen?«

MAG. REINHARD HAIDER,
Amtsleiter Marktge-
meinde Kremsmünster



Es ist ein graues, freudloses Leben, das der britische Autor George Orwell in seinem dystopischen Roman „1984“ beschreibt: Die Welt ist von Krieg zerrüttet. Der 39-jährige Protagonist Winston Smith lebt im totalitär beherrschten England der Zukunft: Eigenständige Gedanken, die freie Kunst und bedingungslose Liebe sind verboten. Überwachung ist allgegenwärtig. Egal ob im Büro, im eigenen Schlafzimmer oder auf der Straße - überall lauschen versteckte Wanzen, überall wird man von vermeintlichen Freund:innen bespitzelt.

Heutzutage wird gerne auf „1984“ verwiesen, wenn von einem bestimmten Land die Rede ist: China. Mithilfe von Gesichtserkennung und digitalen Ausweisen überwacht die Kommunistische Partei jeden Schritt der Chines:innen. In vereinzelten Teilen des Landes werden Social Credit-Systeme erprobt, die von der Partei erwünschte Tätigkeiten belohnen und missfallendes Verhalten bestrafen. Wer einen schlechten Score hat, darf nicht fliegen oder bekommt keinen Job. Menschen, die Widerstand leisten, werden verfolgt und in Umerziehungslagern einer Gehirnwäsche unterzogen. Folter und willkürliche Tötung stehen an der Tagesordnung.

Laut Maximilian Mayer, Professor für Internationale Beziehungen und globaler Technologiepolitik an der Uni Bonn, greift

die Analogie zu Orwells Dystopie dennoch zu kurz: „Der Vergleich hinkt und geht gleichzeitig nicht weit genug. Einerseits gibt es trotz staatlicher Zensur verschiedene Meinungen, die in manchen Teilbereichen auch öffentlich diskutiert werden. Auf der anderen Seite sind wir technologisch auf einem anderen Standpunkt. Es ist viel mehr möglich, als Orwell bedacht hat.“

Auch die Sinologin und Politikwissenschaftlerin Katika Kühnreich warnt vor einer unreflektierten Meinung gegenüber des Reichs der Mitte. Bevor man sich über die Überwachungsstrategie Chinas echauffere, sei es an der Zeit, vor der eigenen Haustür zu kehren: „Man kann im Westen von einem Manipulationskapitalismus sprechen. Große Konzerne wie Facebook und Google sammeln permanent Daten über uns. Sie wollen uns wie einen Esel durch eine Karotte an einer Schnur in die für sie richtige Richtung lenken.“ Als „Mittmach-Überwachungsdictatur“ beschreibt Kühnreich die derzeitige Digitalisierung. Während in Europa persönliche Daten oft unhinterfragt der Privatwirtschaft überlassen werden und sich eher wegen staatlicher Überwachung Sorgen machen, sei es in China genau umgekehrt. Dabei seien alle Menschen durch die Gesellschaft geprägt, in der sie aufgewachsen sind. „Jede:r glaubt, sein/ihr System sei das beste“, sagt Kühnreich. Dabei gebe es



Persönliche Daten sind das Gold des 21. Jahrhunderts.

Wer sie besitzt, weiß häufig mehr über Internetnutzer:innen als sie selbst. Die Frage um Missbrauch dieser Daten gibt es damit seit Anbeginn des Internets.

Während im Westen vor allem Internetkonzerne aus der Privatwirtschaft als Datenkraken gelten, tritt in China der Staat als allwissender Big Brother auf. Wieso wir in einer Gesellschaft der totalen Überwachung leben und jeder Mensch gläsern ist.

TEXT JULIA PABST

DATENMISSBRAUCH - CHINA UND DER WESTEN

BRAVE NEW WORLD vs 1984



zwischen dem Westen und dem Osten einen wesentlichen Unterschied: „Im Gegensatz zu den Europäer:innen und Nordamerikaner:innen sind sich die Chines:innen meistens bewusst, dass sie überwacht werden. Bei uns wird dieser Fakt hingegen gerne ignoriert.“

Westliche Datenkraken

Daten durchdringen unser Leben. Egal ob die per Smartphone bezahlte Pralinenschachtel im Supermarkt, die beim Training vibrierende Smartwatch oder das remote steuerbare Smart Home - alles, was „smart“ im Namen trägt, ist schlau genug, das Verhalten seiner Nutzer:innen zu dokumentieren. Große Internetkonzerne wie Google und Facebook schreiben minutiös mit, was ihre Nutzer:innen tun. Ihre Dienstleistungen sind offenkundig gratis, zumindest monetär gesehen. Beahlt wird im Gold des 21. Jahrhunderts: Daten.

Der Datenschutzverfechter Max Schrems hat bereits 2012 all die Informationen angefordert, die Facebook über ihn gesammelt hat. Heraus kamen 1200 A4-Seiten bedruckt mit höchst privater Information. Chatverläufe, Kommentare und Fotos – auch solche, die der Datenschützer längst gelöscht hat, sind dabei. Würde man die Daten aller Facebooknutzer:innen von 2012 (hochgerechnet von Schrems damaligen Datenbestand) ausdrucken und stapeln, könnte man damit mehr als drei Türme zum Mond bauen. Wie hoch der Stapel wohl fast zehn Jahre später mit knapp dreimal so vielen Nutzer:innen wäre? Facebook dokumentiert jeden Klick, jedes Like, sogar die Verweildauer auf einzelnen Seiten. Aus all den Daten, die wir freiwillig und teilweise unbewusst teilen, erstellen die Facebook-Algorithmen unsere digitale Identität.

Schattenprofile

Standorte, WLAN-Connections und verbundene Adressbücher von Facebook-Freund:innen dienen als Freipass zu privater Information. Dabei müssen Personen gar nicht bei Facebook registriert sein, um ein digitales Profil zu haben. Es reicht schon aus, dass ein:e einzige:r Freund:in sein/ihr Adressbuch mit ►

► Facebook verknüpft – schon hat das soziale Netzwerk sämtliche Telefonnummern, E-Mailadressen und Kontaktfotos abgesaugt. Benutzt werden diese Daten offiziell, um Nutzer:innen miteinander zu verknüpfen. Unter der Rubrik „Personen, die du kennen könntest“ schlägt Facebook potentielle Freund:innen vor. Dabei stehen die vorgeschlagenen Personen immer miteinander – auch noch so entfernt – in Verbindung.

Die Technologiejournalistin Kashmir Hill hat in ihrer Recherche mehrere Anekdoten gesammelt, die zeigen, was durch Schattenprofile möglich wird: Ein Spermaspender, der sein leibliches Kind als Freund vorgeschlagen bekommt. Eine Frau, die mit sechs Jahren von ihrem Vater verlassen wird und 40 Jahre später per Facebook-Freundschaftsvorschlag über sein Profil stolpert. Ein Klient, der seinen Sozialarbeiter nach einem einzigen Treffen unter „Personen, die du kennen könntest“ findet. Und das, obwohl all diese Personen nicht in engerem Kontakt miteinander standen. Das Netz an verbundenen Telefonbüchern und abgesaugten Ortungsinformationen reicht Facebook aus, um Verbindungen herzustellen.

Dass so große Datenschätze in der Hand von einigen wenigen Großkonzernen problematisch sind, zeigte nicht zuletzt der „Cambridge-Analytica-Skandal“. Durch die Weitergabe von persönlicher Information an Dritte wurde immerhin 2016 die Präsidentschaftswahlen in den USA zu Gunsten von Donald Trump beeinflusst. Wie der Philosoph Francis Bacon bereits vor rund 400 Jahren sagte: Wissen ist Macht. In den falschen Händen kann so viel Wissen enormen Schaden anrichten.

IBM und die Nazis

Technologiekritikerin Kühnreich unterstreicht diese Gefahr anhand eines Beispiels aus der Geschichte: „Der Holocaust wäre ohne das Lochkartensystem von IBM nicht in diesem Ausmaß möglich gewesen. Das Vernichtungssystem brauchte eine gut geölte Bürokratie und genaue Datensätze. Immerhin musste von den Zügen bis zum Gaskauf alles organisiert werden.“ Auch die sogenannten Rosa Listen, die im deutschen Kaiserreich des 19. Jahrhunderts geführt wurden, wären für die Nazis ein gefundenes Fressen gewesen. Innerhalb weniger Monate wurden mutmaßlich homosexuelle Männer in Deutschland aufgegriffen, eingesperrt und zum Teil sogar getötet, erzählt Kühnreich. Beim Datenschutz müsse deswegen immer die Zukunft mitbedacht werden, appelliert die Politikwissenschaftlerin: „Daten sterben nicht: Konzernzentralen und Regierungen kommen und gehen, aber die Datensätze bleiben bestehen. Wir wissen nicht, was zukünftige Firmen und Regierungen für Schlüsse aus ihnen ziehen. Wir können nicht sagen, wie sich welche kulturelle Einstellung ändert.“



»Es ist nicht einfach nachzuvollziehen, wie der Social Credit Score genau entsteht und wie man ihn ändern kann. Ich würde es deswegen eher als Überwachungslandschaft als als Überwachungssystem beschreiben.«

MAXIMILIAN MAYER, Junior-Professor für Internationale Beziehungen und globale Technologiepolitik an der Universität Bonn.

Er hinterfragt in seiner Forschung die technische Möglichkeit von Digitalisierungsprojekten durch die Kommunistische Partei Chinas.



»Wir gucken nach China und denken, wir stehen im Trockenen. Aber europäische Werte alleine helfen nicht gegen Überwachung. Es braucht auch politische Handlungen.«

KATIKA KÜHNREICH, Sinologin und Politikwissenschaftlerin

Sie untersucht digitale Überwachung durch die Kommunistische Partei Chinas sowie durch westliche privatwirtschaftliche Konzerne.

Der chinesische Big Brother

Dass Chinas Big Brother, Xi Jinping, bereits heute Menschenrechtsverletzungen unter dem Deckmantel von Sicherheit und Terrorismusprävention versteckt, ist kein Geheimnis. Die Provinz Xinjiang, in der vor allem die unterdrückte muslimische Minderheit der Uigur:innen lebt, sei laut Chinaexpertin Kühnreich ein gigantisches Versuchslabor für allumfassende Überwachung: Die Handys der Einwohner:innen würden regelmäßig von der Regierung gecheckt und zum Teil mit Spionagesoftware versehen, erzählt Kühnreich: „Die Menschen dort können sich der Überwachung nicht entziehen. An Wohnungen etwa gibt es Codes, die man abscanen muss, bevor man eintreten darf. Jede:r Besucher:in muss registriert werden.“

Auch im Rest von China sind Privatsphäre und Meinungsfreiheit Fremdwörter. Tseng Yi-Shuo untersucht von Taiwan aus die digitalen Entwicklungen Chinas: „Den Chines:innen ist Privatheit nicht so wichtig. Sie wissen, dass die Regierung immer zuschaut. Von demokratischen Bemühungen kann keine Rede sein.“

Konnte man früher wenigstens im Internet über ein verschlüsseltes Netzwerk anonym surfen, schiebt auch hier die Kommunistische Partei den Riegel vor: In ganz China müssen Internetnutzer:innen ihren Klarnamen angeben und sich per ID registrieren. Schlimmer noch sei es in einzelnen Testregionen, in denen nur mehr nach einer biometrischen Identitätsprüfung das Internet freigeschaltet werde, erklärt Yi-Shuo: „Früher konnte man zumindest den Ausweis von jemand anderem ausborgen, wenn man nicht wollte, dass der eigene Name auftaucht. Werden hingegen biometrische Daten zur Authentifizierung genutzt, ist für die Regierung ganz klar, wer hinter einem Profil steht.“

Funktionslücken

Vollkommen reibungslos funktioniert das Tracking von digitaler Identität in China aber noch nicht, urteilt Professor Mayer. Zwar werden mittlerweile 90 % der Zahlungen per digitalem Pass über die App WeChat bezahlt, gerade das Social Credit-System sei aber regional sehr fragmentiert. „Es ist kein einheitliches System, sondern mehrere Systeme parallel“, erklärt Mayer. Einzelne Teile seien relativ gut vernetzt: Zum Beispiel gäbe es eine Möglichkeit, Personen auf eine schwarze Liste zu setzen. Über das nationale Gerichtssystem, würde diesen Personen dann zentral die Nutzung von Schnellzügen und Flugzeugen verwehrt. Dann gäbe es aber auch andere Systeme, die viel kleinteiliger seien, sagt Mayer: „Es ist nicht so einfach nachzuvollziehen, wie der Social Credit Score genau entsteht und wie man ihn ändern kann. Ich würde es deswegen eher als Überwachungslandschaft als als Überwachungssystem beschreiben.“



„Wir gucken nach China und denken, wir stehen im Trockenen. Aber europäische Werte alleine helfen nicht gegen Überwachung. Es braucht auch politische Handlungen.“

Die Intransparenz der Algorithmen, die den Social Credit Score berechnen, könne dabei auch zu folgenschweren Fehlern führen, warnt Kühnreich. Mache die Gesichtserkennungssoftware einen Fehler und spiele unteilte Zivile:innen, die gesuchten Personen ähneln, aus, könne das schwerwiegende Folgen haben. Auch die falsche Interpretation von Datensätzen kann zur Verdächtigung von Unschuldigen führen: „Was passiert, wenn Ihre Daten auf einer Terrorliste sind, weil jemand den gleichen Namen hat oder in der gleichen Wohnung gemeldet war wie Sie? Mit diesen Themen werden wir uns zukünftig international auseinandersetzen müssen.“

Sicherheitsproblem

Auch in Punkto Cybersecurity ortet Kühnreich große Gefahr: „Was passiert, wenn private oder staatliche Hacker:innen Ihr Telefon übernehmen und Steuerdaten löschen? Man weiß ja nicht einmal, wie lange es dauert, bis es Ihnen überhaupt auffällt.“ Dieses Problem betreffe China und den Westen in gleichem Ausmaß. Die unterschiedlichen Behörden reagieren aber anders auf die Bedrohung: China versucht sensible Daten in Blockchains zu speichern und Eingriffe von außen dadurch sichtbar zu machen.

In der EU ist Estland Vorreiter in Punkto Digitalisierung und Datensicherheit. Auch hier kommen seit 2012 Blockchains für besonders sensible Daten zum Einsatz. Die meisten Daten werden aber durch eine dezentrale Speicherung geschützt, erklärt Florian Marcus vom e-Estonia Briefing Centre: „Ein bestimmter Datensatz darf nur von einer Behörde angefordert und gespeichert werden. So sind einzelne Server nicht so attraktive Ziele, als dass sich ein riesiger Angriff lohnen würde.“ Der Datenaustausch zwischen den Behörden erfolge verschlüsselt, sagt Marcus: „Die gesamte Plattform ist Open Source, das heißt ihr Quellcode ist online einsehbar. Jeder kann damit auf Schwachstellen hinweisen.“

Schöne neue Welt

Anstatt von einer Reinkarnation von „1984“ zu sprechen, sieht Kühnreich insgesamt den Roman „Schöne neue Welt“ von Aldous Huxley als treffenderes Equivalent zur Gegenwart: „Unsere Gesellschaft ist nicht so trostlos, wie jene die Orwell beschreibt. Viel eher ist sie geprägt von permanenter Ablenkung in Form von Social Media und Konsum.“

In der von Huxley geschaffenen Zukunft geht es allen Menschen augenscheinlich gut: Sexualität wird frei ausgelebt, jede:r hat seinen/ihren fixen Platz in der Gesellschaft und die Glücksdroge Soma sorgt dafür, dass alle glücklich sind. Betrachtet man die schöne neue Welt aber genauer, erkennt man Kratzer in der vermeintlich makellosen Oberfläche: Die Menschen sind in Kästen unterteilt, niemand hinterfragt den Sinn von maßlosem Konsum und partnerschaftliche Liebe existiert nicht. Die Gamification von Apps funktioniere in unserer Welt ähnlich wie die Glücksdroge Soma in Huxleys Roman, meint Kühnreich: „Durch kleine Belohnungen und Benachrichtigungen schütten wir ständig Endorphine aus. Danach werden wir süchtig. Wir sind ständig auf der Suche nach dem nächsten High, ohne zu hinterfragen, wie weit Unternehmen eigentlich gehen dürfen.“

Der Taiwanese Yi-Shuo erkennt in China ein ähnliches Muster. Statt Internetkonzernen hält hier der Staat die Zügel in der Hand: „Die Leute haben online Spaß: Sie kaufen ein oder schauen sich lustige Videos an. Damit hält sie die Regierung bei Laune.“ Es gäbe aber auch klar definierte Grenzen, die nicht überschritten werden dürfen. So sei es beispielsweise verboten, Präsident Xi Jinping zu beleidigen oder die Politik der Kommunistischen Partei zu hinterfragen, sagt Yi-Shuo: „Es gibt hier keinen altmodischen Big Brother, der einem Aussagen im Mund umdreht. Viel eher steckt in den Chines:innen das Bewusstsein, dass sie jederzeit überwacht werden könnten. Sie handeln dadurch anders.“ Dieses Bewusstsein fehle im Westen, mahnt Kühnreich. Auch in Europa müssen sich ihrer Meinung nach Konsument:innen mit der Frage beschäftigen, wie viele Daten sie preisgeben und was mit diesen Daten passiere. Das Credo der Datenschutzexpertin: „Wir gucken nach China und denken, wir stehen im Trockenen. Aber europäische Werte alleine helfen nicht gegen Überwachung. Es braucht auch politische Handlungen.“



»Den Chines:innen ist Privatheit nicht so wichtig. Sie wissen, dass die Regierung immer zuschaut. Von demokratischen Bemühungen kann keine Rede sein.«

TSENG YI-SHUO, Head of the Division of Cyber Warfare and Information Security im Institute for National Defense and Security Research Taiwan

Er untersucht, inwiefern China digitale Technologien zur Überwachung und Unterdrückung der Bevölkerung nutzt und welche Konsequenzen sich daraus für die Meinungsfreiheit ergeben.

Herr Mayer-Schönberger, Sie sind seit Jahrzehnten in der digitalen Welt unterwegs, als Gründer, Professor, Autor, Privatmensch. Machen Sie eigentlich noch einen Unterschied zwischen ihrer analogen und Ihrer digitalen Identität?

Viktor Mayer-Schönberger: Nein. Aber ich habe auch nie in einer digitalen und einer analogen Identität gedacht, sondern immer in Kontext-bezogenen Identitäten. Schon seit den Arbeiten von Goffmann in den 1950ern wissen wir, dass Menschen sich situations- und kontextabhängig verhalten, vor allem auch um das Bild, das andere Menschen sich von ihnen machen, zu beeinflussen. Goffmann verwendete das Bild von Kellnerinnen und Kellnern, die sich gegenüber Gästen anders verhalten als in der Küche - „on stage“ und „backstage“ sozusagen. Und genau das tun wir auch in unterschiedlichen analogen und digitalen Kontexten und bauen damit auch selbst an unseren jeweiligen Identitäten.

Face ID, Facebook-Login, Google-Konto, ID Austria: Für Menschen gibt es heute viele verschiedene Möglichkeiten, sich von Online-Diensten identifizieren zu lassen. Die Anbieter sind sehr unterschiedlich, lassen sich aber in zwei Gruppen einteilen: Staat und Privatunternehmen. Wer wird am Ende die Hoheit über unsere digitale Identität haben? Was präferieren Sie?

Ich denke, ein derartig binärer Blick stellt eher die Sicht als dass er hilft. Es geht ja darum, dass wir Identitätsmechanismen finden, die für die jeweiligen Situationen passen. Also ist es zum Beispiel völlig in Ordnung, für die Anforderung eines Impfsertifikats eine Identitätsmechanismus zu verwenden, der vom Staat getragen wird. Und wenn ich bei Zalando bezahlen möchte, eine privatwirtschaftlich organisierte Identität zu verwenden. Zentral dabei ist: Wir brauchen auch in Zukunft viele unterschiedliche Identitäten, weil wir ja auch in unterschiedlichen Kontexten handeln. Völlig falsch wäre es, wenn wir auf eine einzige Identität hoffen - das wäre ähnlich als würde für unsere sozialen Beziehungen nur mehr

Facebook als Plattform zur Verfügung stellen. Eine gruselige und gänzlich lebensfremde Vorstellung!

Sehen Sie Blockchain und die Krypto-Welt als dritten Weg zwischen Staat und privat?

Nein. Blockchain etc. sind ganz bestimmte technische Mechanismen. Eine Identität (ob analog oder digital) ist anderes und mehr.

Sie haben 2002 das Buch „Machtmaschinen“ veröffentlicht. Wie stark beruht die Macht von Google, Facebook und Co. auf dem Erfassen unserer Online-Identität? Erklärt sich daraus der Rückstand Europas im weltweiten digitalen Wettrennen?

Im Gegenteil! Indem wir in Europa glauben, dass die Macht der digitalen Plattformen darauf beruht, dass sie alles über uns wissen und jedem einzelnen zuordnen können, missverstehen wir die Gefahr der großen Plattformanbieter grundlegend. Und glauben dann auch ganz falsch, sie mit mehr Datenschutzregeln in die Knie zwingen zu können. Die Wahrheit ist: Die großen Plattformen sammeln riesige Mengen an Daten, um daraus statistisch zu lernen, also zu verstehen was jemand, der Produkte A und B und C in dieser Reihenfolge kauft, wahrscheinlich als nächstes kauft. Aber denen ist weitgehend gleichgültig, ob diese Person Viktor Mayer-Schönberger oder Jakob Steinschaden heißt. Die Plattformen lernen also aus Daten, ohne sie bestimmten Identitäten zuzuordnen und daran festzumachen. Wir in Europa haben bis heute nicht verstanden, dass es denen nicht um eine Art Überwachung geht, sondern um eine Art statistisches Lernen (was oft als KI bezeichnet wird). Und deshalb hilft uns bei der Machtbegrenzung der Plattformen auch nicht der Datenschutz, sondern die breite Zugänglichkeit von Daten.

» WIR BRAUCHEN
AUCH IN ZUKUNFT VIELE
UNTERSCHIEDLICHE
IDENTITÄTEN «

JURIST VIKTOR MAYER-SCHÖNBERGER IM GESPRÄCH

INTERVIEW JAKOB STEINSCHADEN



»Die Wahrheit ist: Die großen Plattformen sammeln riesige Mengen an Daten, um daraus statistisch zu lernen, also zu verstehen was jemand, der Produkte A und B und C in dieser Reihenfolge kauft, wahrscheinlich als nächstes kauft.«

VIKTOR MAYER-SCHÖNBERGER
Rechtswissenschaftler



Facebook galt lange als die größte Datensammlung über Menschen und als Nummer-1-Provider digitaler Identität. Nun drängen vor allem Fintechs in den Bereich. Nunmehr gilt das digitale Bankkonto als der Heilige Gral der digitalen Identität. Wird unsere finanzielle Identität zu einem neuen Geschäftsmodell?

Das war sie ja bisher schon. Aus unserer finanziellen Identität leitete sich unsere Bonität ab, und damit die Möglichkeit Transaktionen einzugehen. Was sich wohl ändert in der Zukunft: Es wird leichter werden, unterschiedliche finanzielle Identitäten zu erstellen und zu bewahren. Das ist ein wenig so, als hätten wir viele Kreditkarten zur Verfügung, aus denen wir auswählen könnten, ohne aber für jede dieser Karten wie in der analogen Welt eine hohe Jahresgebühr zahlen zu müssen.

Auch im Gesundheitsbereich werden mit Apps und Gadgets immer mehr Daten erfasst, auch unser Blut wird bald live ausgewertet werden können. Welche neuen Geschäftsmodelle eröffnet das?

Viele - weil wir uns auch dort mehrfache Identitäten zulegen können und werden - für das Sporteln auch gemeinsam mit anderen oder im Wettstreit, für die Interaktionen mit Ärztinnen und Ärzten, etc.

Bei all den Entwicklungen rund um Smart Home, digitalem Eigentum, IoT: Sehen Sie in Zukunft eigentlich überhaupt noch Möglichkeiten, dass wir anonym sein können?

Wir waren ja auch bisher kaum wirklich anonym, sondern hatten eben nur viele Identitäten, die wir in unterschiedlichen Kontexten einsetzen. Solange wir uns diese

Möglichkeit auch im digitalen bewahren, sehe ich kein Problem.

Apple gibt sich seit geraumer Zeit als Verfechter der digitalen Privatsphäre. Kaufen Sie Cupertino das ab?

In einem gewissen Rahmen, ja. Das ist Apples Versuch, sich gegenüber Google und Amazon und Facebook zu differenzieren. Und durch maschinelles Lernen am Gerät (und nicht in der Cloud) und ähnliche Ansätze hat Apple hier Pionierarbeit geleistet. Dass als kommerzieller Anbieter Apple nicht immer maximalen Datenschutz bieten kann, sondern eben auch auf Benutzungsfreundlichkeit oder gesetzliche Grenzen achten muss, verstehe ich. Und, dass es innerhalb von Apple auch intensive Spannungen und laufende Diskussionen über die Interpretation gibt, kann ich auch verstehen - und behalte mir deshalb meinen kritischen Blick bei der Bewertung.

Als Persönlichkeit des öffentlichen Lebens, der bei Politikern, Journalisten oder Wissenschaftlern Gehör findet - müssen Sie sich besonders vor Identitäts-Diebstahl schützen? Wurde schon mal versucht, Sie zu hacken oder zu fälschen?

Ja, natürlich. Da geht es mir wie viele Millionen anderer, deren Daten schon durch Hacks bei Kreditkartenfirmen und Onlineanbietern zugänglich wurden. Und das bedeutete Arbeit, weil Passwörter geändert, Konten gesperrt und Karten ersetzt werden mussten. Ich denke, da müssen wir bei den Strafverfolgungsbehörden mit mehr Personal und mehr Expertise bewusst „aufrüsten“. Damit klar ist, dass Identitäts-Diebstahl kein Kavaliersdelikt ist. ▀

Viktor Mayer-Schönberger ist Rechtswissenschaftler und Professor für „Internet Governance and Regulation“ an der Universität Oxford. Für Deutschland sitzt er außerdem im 2018 geschaffenen Digitalrat der Bundesregierung.

Die Antwort auf die Frage

„Wer bin ich?“, also der Begriff der Identität, ist in der Philosophie seit Jahrtausenden ein immer wieder behandeltes Thema. In Zeiten, in denen immer mehr unserer täglichen Aktivitäten im Internet stattfinden, stellt sich nunmehr auch die Frage nach der digitalen Identität. Es ändert sich zusehends der Identitätsbegriff und wie wir beweisen, wer wir sind. Im realen Leben lässt sich das analoge Selbst etwa mit einem Fingerabdruck oder einem Personalausweis nachweisen, im Internet können sich Menschen anhand ihrer digitalen Identität, mittels E-Mail-Adresse, Benutzernamen und Passwort zu erkennen geben.

Mit der Digitalisierung gewinnt unser digitales „Ich“ jedoch immer mehr an Bedeutung. Wir kaufen online ein, vernetzen uns über soziale Medien wie Facebook, Twitter & Co, tauchen in Spielwelten ein, nutzen Dating-Apps oder erledigen Behördengänge digital. Wir haben also mehrere digitale IDs, die durchaus mehr sind als nur die Datenmengen im Internet. Man könnte sagen, dass wir unsere Identität, durch die Art wie wir online auftreten und welche Informationen wir von uns preisgeben, in die digitale Welt einbringen. Doch bedeutet diese Veränderung der Lebenswelt auch zwangsläufig eine Veränderung unseres Selbst?

Die Merkmale unserer persönlichen Identität, wie Körper, Charakter, Werte, soziale Rollen, unsere Lebensgeschichte und unsere Erfahrungen machen uns als individuelle Menschen aus. Insofern ist es logisch, dass die Digitalisierung, die in unser aller Leben eine wichtige Rolle einnimmt, auch einen Einfluss auf unsere analoge Identität ausübt.

Im Zeitalter multipler Online-Profile, künstlicher Intelligenz, selbstlernender Algorithmen und Roboter müssen wir also auf die Frage der Identität neue Antworten finden. Der Philosoph und Autor Richard David Precht stellt die Frage: „Wer bin ich und wenn ja wie viele?“. Denn unser Auftreten in der virtuellen Welt wird mehr und mehr zum Bestandteil unseres realen Selbstbildes. Digitale und physische Realität verschmelzen immer mehr und müssen daher auch vor Missbrauch geschützt werden. //



» DIE DIGITALISIERUNG WIRD FAST MYTHOLOGISIERT «

LENA PINT, PÄDAGOGIN UND PHILOSOPHIN

Lena Pint ist studierte Pädagogin und Philosophin. Sie hat ihre Doktorarbeit über „Identität im Zeitalter des Internets“ an der Julius-Maximilians-Universität Würzburg geschrieben. Seit 2017 arbeitet die Autorin an einer internationalen Schule in Straßburg.

INTERVIEW JULIA PABST

Was versteht man unter „digitaler Identität“?

Lena Pint: Ich glaube, wir verstehen in einer philosophischen Perspektive etwas ganz anderes unter einer digitalen Identität als diese Datenmengen im Internet, die populärwissenschaftlich damit verknüpft werden. Ich habe mich vor allem mit der Frage beschäftigt, ob wir Identitätsstrukturen noch in derselben Weise denken können durch die Digitalisierung, die alle unsere Lebensbereiche durchdringt. Und digitale Identität habe ich als Gegenbegriff verstanden, in jenem Sinne, dass oft postuliert wird, dass durch die Digitalisierung der Mensch in seinen Identitätsstrukturen umgewälzt wird. „Digitale Identität“ versteht man im philosophischen Diskurs häufig als einen Gegenbegriff zur „analogen Identität“. Es wird unterstellt, dass durch die Digitalisierung die Identität der Menschen nicht mehr mit traditionellen Begriffen beschrieben werden kann. Mit diesem Begriffsverständnis habe ich aber ein Problem: Immerhin wird angenommen, dass wir ein neues Identitätskonzept brauchen, weil wir im digitalen Zeitalter andere Menschen geworden sind. Das sehe ich nicht so.

Wieso?

Wir bringen unsere Identität ins Internet und in digitale Welten ein. Wir verändern sie, wir entwickeln sie weiter. Das heißt aber nicht, dass dadurch die Strukturen meiner Identität komplett wegfallen. Immerhin ist

die analoge Welt gar nicht so anders wie die digitale. Die Digitalisierung wird eben gerne überhoben, ja schon fast mythologisiert. Wir sagen: Wow, Das ist etwas Neues, das verändert unsere Lebenswelt. Da fällt es vielen schwer, einen differenzierten Blick zu bewahren und zu sagen: Leute, ebendiese Phänomene hatten wir vor 20 oder 30 Jahren schon genauso in der analogen Welt. Jetzt kommen sie lediglich deutlicher zum Vorschein.

Meine Kritik setzt eben daran an, dass wir diesen Bruch zwischen digitaler und analoger Welt so nicht aufrechterhalten können. Wir brauchen diese Unterscheidung nicht. Wir können uns als Menschen in unserer Identität immer noch mit den althergebrachten analogen Begriffen beschreiben und die aufs Internet umsetzen. Das ist kein Gegensatz.

Sie sprechen da das Zusammenspiel zwischen digitaler und analoger Identität an - das ist ja irgendwo eine Einheit und doch etwas Eigenständiges. Kann man das vielleicht mit der philosophischen Frage nach dem Zusammenspiel zwischen Körper und Geist vergleichen?

Diese seltsame Trennung von Körper und Geist, die da postuliert wird, als wären wir reine Geistwesen, die zufällig einen Körper haben, die ist im Grunde gar nicht so erfüllbar. Die kommt uns kulturhistorisch ►

„Wir können uns als Menschen in unserer Identität immer noch mit den althergebrachten analogen Begriffen beschreiben und die aufs Internet umsetzen. Das ist kein Gegensatz.“





► und philosophiehistorisch so logisch vor, tatsächlich nehmen wir uns sehr wohl als Einheit wahr: Ich habe einen Körper, ich bin ein Leib. Mein eigenes Körperempfinden wäre dann die Leiblichkeit. Wenn Sie da die Analogie zur digitalen und analogen Identität ziehen möchten, könnte man schon sagen, dass man Ähnlichkeiten finden kann. Nämlich insofern, als dass unsere Identität ebenfalls nicht geteilt ist in eine digitale und eine analoge.

Wir bringen unsere Identität ins Internet und in digitale Welten ein. Wir verändern sie, wir entwickeln sie weiter. Natürlich bieten digitale Welten einen ganz spezifischen situativen Rahmen. Das heißt aber nicht, dass dadurch die Strukturen meiner Identität wegfallen würden. Ich würde da gar nicht so streng unterscheiden. Ich glaube, diese vermeintliche Trennung hat auch viel damit zu tun, dass die Digitalisierung so überhoben, ja schon fast mythologisiert wird. So à la: Das ist etwas neues, wow, das verändert unsere Lebenswelt. Da fällt es schwer, einen differenzierten Blick zu bewahren und zu sagen: Leute, diese Phänomene hatten wir vor 30 Jahren schon genauso in der analogen Welt. Wie gesagt: Jetzt kommen sie vielleicht deutlicher zum Vorschein, so ganz neu sind sie aber auch nicht.

»Dass die Algorithmen unsere Identität nicht greifen können, ist ihnen egal. Es interessiert sie nicht, warum wir etwas tun, ob wir eine Hose aus Impuls kaufen oder ob wir diese Marke aus tiefsten Herzen unterstützen. Es geht ihnen lediglich darum, unser Kaufverhalten vorherzusehen. Unsere Identität ist dadurch nicht bedroht.«

LENA PINT

Sprechen wir über die Körperlichkeit im digitalen Raum. Welche Rolle spielt der Körper auf Social Media und Co.?

Als das Internet massentauglich wurde, wurde es als Ort gepriesen, wo das Aussehen keine Rolle spielt, wo ich meinen Körper zurücklassen kann und wo er nicht relevant ist. Das ist aber durch das Web 2.0 in sein Gegenteil verkehrt worden: Hier ist das Äußerliche sehr wohl relevant, hier sind die körperlichen Darstellungen durch die Selfiekultur auf Social Media sogar omnipräsent. Selbstverständlich werden Körperbilder da oft retuschiert, man möchte sich selbst in einem guten Licht darstellen. Das unterstreicht auch die Bedeutung, die der Körper für unsere Identität hat und immer hatte. Das ist nichts Neues. Ich finde, das weist in einer besonderen Weise auf die Bedeutung

unserer Körperlichkeit hin. Die hat sich ganz entgegen der Prognosen von den Anfängen des Internets nicht geschmälert, sondern sogar verstärkt.

Inwiefern kommen bei dieser digitalen Selbstdarstellung alte Strukturen zu tragen?

Als Mark Zuckerberg Facebook gegründet hat, hat er gesagt, Facebook würde unsere sozialen Rollen aufheben. Immerhin gibt es hier nicht diese klassische Trennung zwischen Arbeit und Privatleben. Wir sind dort mit unserer Mutter, mit Arbeitskolleg:innen und mit Kindheitsfreund:innen befreundet. Das sind sehr unterschiedliche Menschen, die verschiedene Rollenvorstellungen an uns herantragen.

Diese Erwartungen fallen entgegen Zuckerbergs Prognose in der Realität aber nicht weg. Viele Leute reagieren auf diese vielen unterschiedlichen Erwartungen, indem sie eine Minimalrolle einnehmen. Sie überlegen sich ganz genau, was sie posten und posten dann Inhalte mit einem minimalen Konsens. Zum Beispiel: Ich bin gegen Rassismus oder ich gehöre der Gruppe der Langschläfer:innen an. Das kann jemand blöd finden, aber diese Inhalte sind generell nicht sonderlich aufregend. Die meisten Facebookprofile sind tatsächlich ziemlich langweilig. Den Leuten ist eben sehr wohl bewusst: Meine Mama mag das vielleicht nicht, wenn ich ein Bikini-foto von mir poste.

Wir hinterlassen online auch unbewusste Spuren: Wie lange wir ein Foto anschauen, was wir liken, was wir skippen. Führen diese Aufzeichnungen über unser Verhalten dazu, dass wir zu gläsernen Menschen werden?

Das sicherlich! Gerade diese Personalisierungstendenz der Werbung kann problematisch werden: Wenn ich gerade schlecht gelaunt bin, flasht dann vielleicht eine Anzeige für Schokolade auf, die ich in dem Moment unbedingt haben will und ich kaufe sie. Da werden evaluative Prozesse manipuliert.

Es ist auch eine Frage der Kontrolle: Eine Frage, ob ich kontrolliere, welche Daten da ins Internet fließen und welche nicht. Gleichzeitig konnte ich das im Analogen aber auch nicht kontrollieren, wie mich jemand beobachtet und auf welchen Fotos ich im Hintergrund zu sehen bin. Ich wusste auch hier nicht, welche Spuren ich wo hinterlasse. Im Internet erleben wir eine Zuspitzung dieser Dinge und ich verstehe, dass das auch überwältigend sein kann. Gerade durch diese

»Als das Internet massentauglich wurde, wurde es als Ort gepriesen, wo das Aussehen keine Rolle spielt, wo ich meinen Körper zurücklassen kann und wo er nicht relevant ist. Das ist aber durch das Web 2.0 in sein Gegenteil verkehrt worden.«

LENA PINT

Datenmengen, auf die so unglaublich viele Leute potenziell Zugriff haben.

Neu sind zudem die Algorithmen, die die Daten verarbeiten: Man wird auf Basis dieser Algorithmen in Kategorisierungen gesteckt. Das hat so etwas Gesichtsloses. Und ich glaube, das trägt zur Angst vieler Menschen bei, dass diese Algorithmen viel mehr über mich wissen, als ich preisgeben wollte.

Kann man in diesem Sinne von einer Entmenschlichung sprechen?

So weit würde ich nicht gehen. Selbstverständlich war der Algorithmus noch nie menschlich. Aber wir werden dadurch nicht unmenschlich. Wir werden nur unmenschlich, wenn wir uns auf unsere digitalen Daten reduzieren lassen. Auch wenn wir unglaubliche Datenmengen im Internet hinterlassen, sind wir viel mehr als das. Wir kommen als leiblicher Mensch im Internet nicht vor.

Aber reduzieren uns private Konzerne nicht eben auf unsere Daten, indem sie Verhalten in Nullen und Einsen darstellen und uns dadurch in Kategorien einordnen?

Doch, sicherlich, und damit haben sie auch Erfolg. Nur bezweifle ich, dass sich meine Identität in irgendeiner Form als Datenmenge beschreiben lässt: Sie ist viel zu komplex. Wir hinterlassen im Internet nie all jene Informationen, die uns zum Menschen machen. Ich bin keine Anordnung von Daten. Ich bin zum Beispiel nicht schüchtern, ängstlich oder introvertiert, sondern mein Charakter ist eine Vernetzung von verschiedenen Dispositionen in unterschiedlichen Abstufungen.

Dass die Algorithmen unsere Identität nicht greifen können, ist ihnen aber egal. Es interessiert sie nicht, warum wir etwas tun, ob wir eine Hose aus Impuls kaufen oder ob wir diese Marke aus tiefstem Herzen unterstützen. Es geht ihnen lediglich darum, unser Kaufverhalten vorherzusehen. Unsere Identität ist dadurch nicht bedroht. Was uns das Internet aber sehr wohl zeigt, ist, dass wir weniger überraschend sind, als wir denken. Unser Verhalten ist vorhersehbar. Aber trotzdem: Unsere Identität ist und bleibt etwas Individuelles. ▀



IDENTITÄT IM ZEITALTER DES INTERNETS
Lena Pint

Die Lebenswelt des heutigen Menschen ist von einer zunehmenden Digitalisierung geprägt, die viele Autor:innen zu einem Infragestellen traditioneller Identitätskonzepte veranlasst. Die daraus resultierende Vorstellung einer genuin „digitalen Identität“, die das Wesen der Menschen von nun an bestimme, wird in dieser Arbeit kritisch betrachtet.

Königshausen & Neumann
€ 49,80

Wie wird eine digitale Identität unseren Identitätsbegriff verändern bzw. hat sich dieser bereits mit dem Internet in den vergangenen Jahren verändert?

Konrad Paul Liessmann: In der Tat, man kann diesen Eindruck haben. Aber nur unter der Voraussetzung, dass wir mit dem Begriff der Identität eher sorglos umgehen. Identität heißt Sichselbstgleichheit. Strenggenommen können wir nicht mehrere Identitäten haben, außer wir könnten uns in mehrere getrennte Personen aufspalten. Damit diese sich aber als Einheit begreifen – „Das bin doch auch ich“ – müssen wir eine übergeordnete Identität annehmen, unter der sich diese verschiedenen Subidentitäten wieder versammeln. In der älteren Soziologie sprach man von unterschiedlichen beruflichen, sozialen, sexuellen, kulturellen Rollen, die Menschen spielen können. Mir scheint das noch immer etwas angemessener als der modische Begriff der Identität. Aber wir müssen nun einmal mit diesem leben.

Bewirkt eine Veränderung des Identitätsbegriffes nicht auch eine komplette Veränderung unseres Lebens?

Nun, niemand kann sich vollständig ändern. Damit ich weiß, dass ich mich geändert habe, muss es zwischen der alten und der neuen Identität eine Verbindung geben. Man schlüpft ja nicht in die Haut eines anderen Menschen, sondern ändert einige Eigenschaften, Verhaltensweisen, Konsumvorlieben und Einstellungen. Aber alles, was man war und erlebt hat, schleppt man auch in der vermeintlich neuen Identität mit sich.

Darf man hier optimistisch sein, dass eine digitale Identität Menschen besser macht oder muss man sich vor den Folgen eher fürchten?

Die digitale Identität erlaubt nun allen Menschen, was früher nur einer privilegierten Schicht vorbehalten war: Sich in einer ganz bestimmten Weise einer Öffentlichkeit oder sozialen Gruppe zu präsentieren. Das macht uns nicht auf Anhieb besser, denn man kann im digitalen Raum auch mit der Identität eines Killers, Dschihadisten oder Hassposters kokettieren. Interessanterweise nehmen wir solche Identitäten, wenn wir ihnen auf Social Media begegnen, sofort für bare Münze und gehen mit Gesetzeskraft dagegen vor. Wir sagen ja nicht: Ach, der hat sich halt spielerisch die digitale Identität eines Hassposters zugelegt, ansonsten ist er ja ein netter Mensch.

Digitale Identitäten geben uns auch neue Freiheiten. Damit können wir in Zukunft quasi auf Knopfdruck unsere Identität ändern und unterschiedlichste Bedürfnisse ausleben. Kann uns das nicht glücklicher machen?

So einfach ist es nicht. Und auf Knopfdruck geht gar nichts, das ist ein Mythos.

Sich eine neue Identität zuzulegen, die auch glaubwürdig sein soll, erfordert harte Arbeit, ständige Kontrolle des Bildes, das ich von mir entwerfe, und der Reaktionen, die ich darauf bekomme. Und dann ist es uns gerade in den sozialen Medien zunehmend verwehrt, beliebige Identitäten auszuprobieren. Da gibt es strenge Regeln. Wer mit einem Knopfdruck sich etwa eine andere Hautfarbe zulegt und als Angehöriger einer anderen Ethnie ausgibt, kommt schnell in den Verdacht, rassistisch zu denken und kulturelle Aneignung zu betreiben. Die Freiheit ist auch im Netz alles andere als grenzenlos.

Gilt es nicht auch zu klären, wem das digitale ICH gehört?

Durchaus. Das digitale Ich besteht aus Datenströmen, und diese werden von Digitalunternehmen generiert, kontrolliert, gesichert, aufbewahrt und verwertet. Wem Twitter oder Facebook den Account sperren, der ist plötzlich nichts mehr – auch wenn er vorher Präsident der USA war. Aber das war schon in der vordigitalen Antike so. Schon der stoische Philosoph Epiktet sagte, dass über vieles an uns – vom Ansehen, das wir genießen, bis zum Körper – andere verfügen können. Vieles liegt nicht in unserer, sondern in einer anderen Macht. Eine Identität jedoch, die so abhängig von anderen ist, ist keine Identität. Denn letztlich wäre ich dadurch durchgängig fremdbestimmt.

Würde mit einer gesellschaftlichen Legitimierung eines digitalen ICHS die Grenze zwischen Mensch und Maschine verschwimmen?

Ich bin vorsichtig mit solchen Prognosen. Zum Identitätsgefühl gehört eine Form des Selbstbewusstseins, die ich bei KI noch nicht sehe. Ich möchte aber auch nichts kategorisch ausschließen. Aber vorrangig scheint mir allemal die Frage zu sein, wer wir sein wollen, das heißt: Welches Leben wir führen wollen. Maschinen führen (noch) kein Leben.

Was erscheint Ihnen persönlich als die zentrale Frage, die im Rahmen der digitalen Identität beantwortet werden sollte?

Mir scheint es spannend zu beobachten, wie sich die vermeintliche digitale Identität auf das tatsächliche Lebensgefühl der Menschen auswirkt, vor allem, wenn deutlich wird, dass wir mit den selbst entworfenen digitalen Ebenbildern nicht mithalten können. Das Gefühl, dass dann eine Identität einer anderen nachhinkt, wird die Menschen noch depressiver machen als sie schon sind. Meine Vermutung: Es wird bald Aufstände gegen die digitalen Identitäten und eine Feier des Lebens in der natürlichen Unmittelbarkeit geben. ▀

Der Philosoph Univ. Prof. Dr. Konrad Paul Liessmann spricht im Interview über den neuen Identitätsbegriff, die vermeintliche Freiheit des Internets und das Problem, dass Menschen mit ihrem eigenen digitalen ICH nicht mehr mithalten können.

INTERVIEW
STEPHAN SCOPPETTA

A portrait of Prof. Dr. Konrad Paul Liessmann, a middle-aged man with grey hair and glasses, wearing a dark suit and tie. He is seated and looking directly at the camera with a serious expression. The background is a blurred interior space with a statue visible on the left.

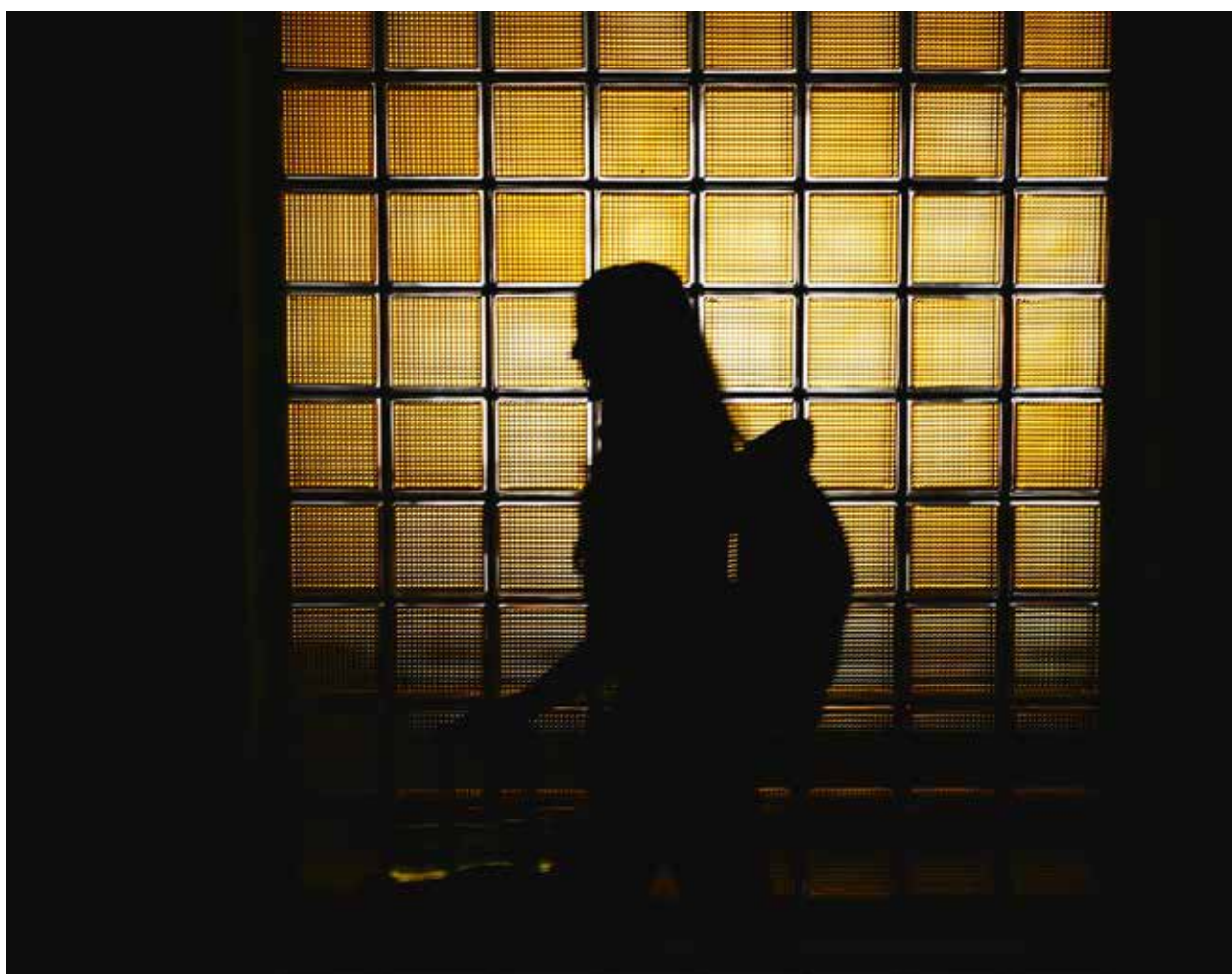
**» SICH EINE NEUE
GLAUBWÜRDIGE
IDENTITÄT ZUZULEGEN,
ERFORDERT
HARTE ARBEIT «**

PHILOSOPH UNIV. PROF. DR. KONRAD PAUL LIESSMANN

EUROPÄER:IN ODER ÖSTERREICHER:IN?

Was schafft eine nationale Identität? Der Ort der Geburt ist Umfragen zufolge gar nicht so wichtig, vor allem die gemeinsame Sprache gilt als identitätsstiftend. Auch gemeinsame Werte und Traditionen werden als wichtig angesehen, die Religionszugehörigkeit dafür weniger. In den einzelnen Staaten gibt es allerdings teils deutliche Unterschiede. Im Jahr 2019 gaben rund 21 Prozent der Befragten in Deutschland im Alter zwischen 16 und 26 Jahren an, dass sie sich selbst nur als Bürger:in des eigenen Landes sehen. In Großbritannien lag dieser Wert bei rund 41 Prozent. *

Quelle: Statista



IMPRESSUM

Die in dieser Ausgabe veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung und Speicherung in Datenverarbeitungsanlagen nur mit ausdrücklicher Genehmigung des Herausgebers. Zitate aus Beiträgen dieser Ausgabe sind ausschließlich mit Angabe der Quelle gestattet. **Herausgeber** Trending Topics GmbH, Liechtensteinstraße 111/115, A 1090 Wien
Geschäftsführung Bastian Kellhofer **Anzeigen** Bastian Kellhofer **Chefredaktion** Oliver Janko **Art Director** Željko Bašura **Photo Director** David Visnjic
Redaktion Helene Tuma, Gerrit Gubo, Alois Pumhösel, Sandra Wobrazek, Stephan Scoppetta, Oliver Janko, Jakob Steinschaden
Produktion Red Sam Media GmbH **Fotos & Illustrationen** Shutterstock, younix AG /OSD/Wilke, Barracuda Networks, David Visnjic, WKÖ/Studený, Ossbig, Lena Pint, Anyline, Swilox, VID, NetID, Viktor Mayer-Schönberger, Handelsverband/Doleschal, CRIF, niceshops, Heribert Corn, BMDW, PSA.
Sofern nicht anders angegeben liegen die Bildrechte bei den jeweiligen Unternehmen, NGOs, Organisationen und Privatpersonen.
Wir bedanken uns für die Nutzungsmöglichkeit! **Mails** feedback@trendingtopics.at



Building a better
working world

Verändern Sie Algorithmen oder verändern Sie?

Der digitale Wandel verändert die Art,
wie Unternehmen handeln. Sie sollten alle
Chancen nutzen, die die Digitalisierung für
nachhaltiges Wachstum bietet.

ey.com/at/digital #BetterQuestions



The better the question. The better the answer.
The better the world works.

Digitale Identität – einfach sicher identifizieren



Sicherheit beginnt mit der digitalen Identität. Wir machen es für Ihre Online-Kunden sicher und einfach convenient. Als Identification Hub sind wir Ihre Verbindung zu den gängigsten Identifikations-Verfahren – mit nur einer Schnittstelle maximale Abdeckung. Ihre Kunden wählen selbst, mit welcher Identifikations-Methode sie ihre digitale Identität bestätigen möchten – **einfach sicher, medienbruchfrei und regelkonform.**

Wir setzen neue Maßstäbe für mehr Sicherheit im Online-Business.
Sicher mit CRIF, dem führenden Identification Service Provider in Europa.