Christian Aretz

Der Souverän in der Krise

Gedanken zur Reichweite der Macht über die eigenen Identitätsdaten

Kann Souveränität über die eigene digitale Identität ausgeübt werden? Welchen Beitrag zur Datensouveränität leisten bewährte und neue Technologien für die Identitätsverwaltung? Und was hat Datenschutz eigentlich damit zu tun? Ein Rückblick, ein Ausblick und eine Streitschrift.

1 Zum Begriff der Souveränität

»Das Bier ist kein Bier, was dadurch ausgeglichen wird, daß die Zigarren keine Zigarren sind, aber der Paß muß ein Paß sein, damit sie einen in das Land hereinlassen.«
(B. Brecht „Flüchtlingsgespräche")[1]

Der Begriff „Datensouveränität" wurde, insbesondere hinsichtlich seiner juristischen Einwertung, in der Vergangenheit bereits vielfach diskutiert – mit bislang uneindeutigem Ergebnis.[2] Er ist dabei wahrlich keine neue oder moderne Wortschöpfung, wird jedoch rapide zunehmend, je nach politischer Agenda oder ökonomischer Zielsetzung, jenseits der Rechtsdogmatik und häufig zu reißerischen Marketingzwecken verwendet und lädt zu verschiedensten Interpretationsmöglichkeiten ein. Mal soll er glauben lassen, eine bestimmte Lösung oder ein Produkt leiste einen herausragenden Beitrag zu dem nicht minder antiquierten Recht auf informationelle Selbstbestimmung,[3] mal soll er umfangreiche Kontroll- und Prüfmöglichkeiten der Datenverarbeitungen herausstellen,[4] und nicht zuletzt taucht er als „Buzzword" im öffentlichen politischen Diskurs auf, z. B. im Rahmen des Projekts "Digitale Identitäten" der Bundesregierung.[5] Hatte man in der Welt des Thomas Hobbes die Souveränität noch als uneingeschränkte Allmacht verstanden, weicht der aktuelle Diskurs den Begriff auf und lässt ihn zu einem Kalenderspruch verkommen. Anzumerken sei bereits an dieser Stelle, dass ein staatsrechtlich gemeinter Souveränitätsbegriff im Lichte des europäischen Datenschutzrechts schon alleine deswegen irreführend wäre, da das Konstrukt eines unumschränkten Dateneigentums die Rechte und Pflichten der datenschutzrechtlich Verantwortlichen und Dritter verletzen, und öffentlichen Interessen regelmäßig zuwider laufen würde.[6] Es ist mithin nicht überraschend, dass der Souveränitätsbegriff weder in der DSGVO, noch in ihren Erwägungsgründen genannt wird.

Eine Besonderheit stellt in diesem Zusammenhang die nunmehr kreierte Wortschöpfung der „selbstsouveränen Identität" (Self-Sovereign Identity, abgekürzt: SSI) dar. Hinter dieser semantischen Redundanz verbirgt sich eine dezentrale, in der Regel auf Blockchain-Technologie basierte, Identitätsverwaltung.[7] Sie kommt regelmäßig ohne zentrale staatliche Stellen oder Vermittler aus, wodurch es ermöglicht wird, dass eine Person ein digitales Surrogat ihrer Identität selbst erstellt und fürderhin selbst

1 Alle den Kapiteln vorangestellten Zitate, soweit nicht anders gekennzeichnet, entstammen dem Werk „Flüchtlingsgespräche" von Bertold Brecht, erschienen im Suhrkamp Verlag Berlin, 6. Auflage 2019 (suhrkamp taschenbuch 3129).

2 Sehr ausführlich dazu *Martini/Kolain/Neumann/Rehorst/Wagner*, Datenhoheit, MMR-Beil. 2021, 3.

Christian Aretz

ist Experte für deutsches und europäisches Datenschutzrecht, Informationssicherheitsstandards und Managementsysteme. Er ist Geschäftsführer der VP Data Protection GmbH und seit über 20 Jahren als Berater und Beauftragter für Informationssicherheit und Datenschutz tätig. Im IAPP Exam Development Board entwickelt er Lernmaterialien und Prüfungsfragen für Datenschutz-Zertifizierungsprogramme und ist selbst zertifiziert als CIPP/E, CIPM, CIPT, FIP, CISM, CISA und ISO/IEC 27001 Senior Lead Implementer.
E-Mail: christian.aretz@vpdata.de

3 *Ehrlich, T., Richter, D., Meisel, M. et al.*: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. HMD 58, 247–270 (2021).

4 *Hummel/Braun/Augsberg/von Ulmenstein/Dabrock*: Datensouveränität, Springer VS, Wiesbaden, 2021. Abrufbar unter https://link.springer.com/content/pdf/10.1007%2F978-3-658-33755-1.pdf.

5 Details zum Projekt abrufbar unter https://www.bmi.bund.de/Webs/PA/DE/verwaltung/projekt_digitale_identitaeten/projekt_digitale_identitaeten_node.html.

6 *Braun/Hummel/Dabrock/Veil*: Datensouveränität (PK.29 der Dataprotection-Landscape), abrufbar unter https://dataprotection-landscape.com/law/policy-concepts/data-sovereignty.

7 *Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F.* (2021): Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Abrufbar unter: https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf.

verwaltet.[8] Mit der Förderung des Bundesministeriums für Wirtschaft und Energie (BMWi) wurde ein auf diesem Konzept basiertes Modell entwickelt, welches in Form der digitalen ID Wallet der Bundesregierung Gestalt angenommen hat. Solche nutzerzentrierten Lösungen sollen Bürgern zu einem selbstbestimmten Umgang mit der eigenen digitalen Identität verhelfen.[9] Zentrale Komponente dabei soll eine selbst erstellte digitale Identität sein, welche mit Hilfe der eID-Funktion des Personalausweises verifiziert und auf dem Smartphone hinterlegt wird.

2 Der Ausweis als Identitätsnachweis

»Der Paß ist der edelste Teil von einem Menschen. Er kommt auch nicht auf so einfache Weise zustand wie ein Mensch. Ein Mensch kann überall zustandkommen, auf die leichtsinnigste Art und ohne gescheiten Grund, aber der Paß niemals. Dafür wird er auch anerkannt, wenn er gut ist, während ein Mensch noch so gut sein kann und doch nicht anerkannt wird.«

(B. Brecht „Flüchtlingsgespräche")

Der Pass dient in erster Linie dem Nachweis über die eigene Identität. Seit dem Mittelalter existieren entsprechende Dokumente in Papierform,[10] in unserer heutigen Lebensrealität kennen wir sie in Form von Kunststoffkarten oder, im Falle des Reisepasses, als gebundenes Büchlein.

Ausweisdokumente, wie z. B. der Personalausweis oder der Reisepass, werden vom Staat an den Bürger ausgegeben. Zwar hält dieser ihn sodann in eigener Verwahrung, jedoch verbleibt das Eigentumsrecht über das Dokument aus völkergewohnheitsrechtlichen Gründen beim ausstellenden Staat.[11] Der Ausweis darf grundsätzlich nicht eingezogen werden, es existieren jedoch zahlreiche Ausnahmen von dieser Regel.[12] Auch kann die Ausstellung eines Passes gemäß § 7 PaßG gänzlich versagt werden, wenn einer der darin genannten Versagungsgründe vorliegt. Insofern muss erheblich bezweifelt werden, dass überhaupt eine Souveränität über die dokumentierte Identität, zumindest aber über das physische Ausweisdokument ausgeübt werden kann.

3 Souveränität in einer ID-Wallet

»Man kann sagen, der Mensch ist nur der mechanische Halter eines Passes. Der Paß wird ihm in die Brusttasche gesteckt wie die Aktienpakete in das Safe gesteckt werden, das an und für sich keinen Wert hat, aber Wertgegenstände enthält.«

(B. Brecht „Flüchtlingsgespräche")

Eine Brieftasche (in die englische Sprache übersetzt: Wallet) dient der Aufbewahrung von Fahrerlaubnis- und Ausweisdokumenten, Mitglieds-, Geld- und Kreditkarten und nicht zuletzt auch von Bargeld. Dies alles an einem Ort gesammelt verfügbar zu halten, empfinden wir als komfortabel, messen einem derartigen Konglomerat von wichtigen und wertvollen Gegenständen im Lebensalltag eine entsprechend hohe Bedeutung zu und sind im Umgang damit in hohem Maße sensibel. Ihr Verlust verursacht hingegen nicht nur enorme organisatorische, zeitliche und finanzielle Aufwände bei der Wiederbeschaffung der Dokumente, sondern kann einem unredlichen Finder die nötigen Grundlagen für einen Identitätsdiebstahl verschaffen. Insofern trägt der Besitzer einer Brieftasche eine enorme Verantwortung für ihre Verfügbarkeit und Integrität.

Mit der Idee einer digitalen ID-Wallet soll das Prinzip der Dokumentensammlung in einer Brieftasche auf Initiative der Bundesregierung in die digitale Welt transformiert werden.[13] Ein europaweiter Ansatz findet sich in Art. 6a des eIDAS-ÄVO-V,[14] in dessen Abs. 7 dem Nutzer die uneingeschränkte Kontrolle über die sog. EUid-Wallet und die darin hinterlegten Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen zugesichert wird. Damit werden bedeutsame Anforderungen an eine physische Brieftasche auf die digitale Wallet übertragen: Die Dokumente sollen beim Besitzer verbleiben (Prinzip der Dezentralität), sie sollen nicht ohne sein aktives Zutun gespeichert, ausgewählt, kombiniert und weitergeben, ausgelesen oder übertragen werden können (Zugriffsschutz). Außerdem soll es ermöglicht werden, dass nur einzelne Dokumente, und daraus sogar nur einzelne Datenkategorien, freigegeben und übertragen werden können (Prinzip der Datenminimierung).

Von besonderer Bedeutung ist auch die Gewährleistung von Echtheit und Fälschungssicherheit der Dokumente. Physische Ausweisdokumente verfügen über physische Sicherheitsmerkmale (z. B. mehrfarbige Guillochen, Mikroschriften, holografische Elemente, personalisierte Sicherheitsfäden), welche jederzeit – und häufig auch ohne technische Hilfsmittel – überprüft werden können. Digitale Ausweisdokumente müssen gleichermaßen echt, fälschungssicher und in der digitalen Welt zudem unabstreitbar sein. Um dies zu gewährleisten, braucht es einen Vertrauensanker, wofür sich seit Jahrzehnten Public-Key-Infrastrukturen grundsätzlich bewährt haben und als Goldstandard gelten dürften. Diese stehen seit langer Zeit zur Verfügung und werden auch zu hoheitlichen Zwecken genutzt. Die Bundesrepublik Deutschland ist dafür Ende 2007 dem Public Key Directory (PKD) der International Civil Aviation Organization (ICAO) beigetreten.[15] Mit Hilfe dieses Verzeichnisses werden seitdem international Pässe und andere Reisedokumente geprüft. Eine Nutzung dieser Infrastruktur wäre auch für andere digitale Identitäten leicht und gewinnbringend, ohne dabei den Spagat mit neuen, unbekannten und nachweislich ungeeigneten Technologien machen zu müssen.

Dass im Rahmen der digitalen ID-Wallet der Bundesregierung als Vertrauensanker jedoch ausgerechnet eine Blockchain-basierte Lösung ausgewählt wurde, ist Teil einer äußerst kontrovers geführten Diskussion. Blockchaintechnologie gilt als hochkomplexe (und daher potenziell unsichere) Technologie, die den Experi-

8 *Guggenberger*, MAH IT-R, Teil 14.2 Blockchains Rn. 23.

9 Vgl. https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/SchaufensterSichereDigIdentProjekte/sdi-projekt_ssi.html.

10 *Hartmann*, Geschichte Italiens im Mittelalter. Bd. II Teil 2, Perthes, Gotha 1903, S. 147–148.

11 *Beimowski/Gawron* in Beimowski/Gawron PaßG § 1 Rn. 15.

12 *Winkelmann/Kolber* in Bergmann/Dienelt AufenthG § 3 Rn. 6, sowie *Beimowski/Gawron* in Beimowski/Gawron PaßG § 8 Rn 3.

13 Details zu diesem Vorhaben unter https://www.bundesregierung.de/breg-de/suche/e-id-1962112.

14 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0281&from=DE.

15 Liste der teilnehmenden Staaten abrufbar unter https://www.icao.int/Security/FAL/PKD/Pages/ICAO-PKDParticipants.aspx.

mentierstatus noch nicht überwunden hat.[16] So mussten bereits unmittelbar nach der Veröffentlichung der ID-Wallet App Teile der zu Grunde liegenden Infrastruktur abgeschaltet werden – das System steht seitdem nicht mehr zur Verfügung[17]. Diesem Schritt gingen umfangreiche Untersuchungen seitens prominenter IT-Sicherheitsexperten voraus, welche die enormen Nachteile dieser Technologie und, ganz konkret, auch die vorliegende technische Umsetzung der digitalen ID-Wallet bemängelt hatten.[18]

In diesen Untersuchungen konnte z. B. nachgewiesen werden, dass auf Grund von Konfigurationsfehlern eine Verfügbarkeit zentraler Systeme nicht durchgängig gewährleistet war. Dies überrascht umso mehr, als dass eine Blockchain-basierte Lösung üblicherweise ohne solche zentralen Systeme operiert.[19]

Wann immer zentrale Systeme Teil einer konzeptionellen Lösung sind, muss damit gerechnet werden, dass sie nicht verfügbar, kompromittiert oder anderweitig dysfunktional sind und eine korrekte Identifizierung somit nicht möglich ist.

16 So die Auffassung des BSI in seiner Bewertung des Hotel Check-in Piloten, S. 6, abrufbar unter https://media.frag-den-staat.de/files/foi/640187/bewertung_hotel_checkin_pilot.pdf.

17 Stand: 03.11.2021.

18 *Biselli*, Konzeptionell kaputt und ein riesiger Rückschritt, abrufbar unter https://netzpolitik.org/2021/interview-zu-id-wallet-konzeptionell-kaputt-und-ein-riesiger-rueckschritt.

19 Details dazu im CR272 „Wie die Union ihren Internetführerschein verlor" (14.10.2021), abrufbar unter https://chaosradio.de/cr272-id-wallet.

Allein auf Grund der technischen Abhängigkeit von Dritten und dem mit der Nichtverfügbarkeit einhergehende Kontrollverlust muss bezweifelt werden, dass im Rahmen der digitalen ID-Wallet eine Souveränität über das Identifizierungsmittel überhaupt ansatzweise ausgeübt werden kann.

4 Souveränität bei der Identifizierung

»Und doch könnt man behaupten, daß der Mensch in gewisser Hinsicht für den Paß notwendig ist. Der Paß ist die Hauptsach, Hut ab vor ihm, aber ohne dazugehörigen Menschen wär er nicht möglich oder mindestens nicht ganz voll«

(B. Brecht „Flüchtlingsgespräche")

Die ID-Wallet App der Bundesregierung arbeitet, ähnlich wie dies bei den bereits in unserem Lebensalltag angekommenen Apps zur Speicherung des „Digitalen COVID-Zertifikat der EU" der Fall ist, mit QR-Codes. Solche Codes bilden die in ihnen hinterlegten Daten binär in maschinenlesbarer Form ab, woraus folgt, dass sie im Rahmen einer bloßen Sichtprüfung keinerlei durch einen Menschen interpretierbare Information preisgeben.

Anders als bei den Apps zur Eindämmung der COVID-19-Pandemie, wo die Verifizierung der in den QR-Codes hinterlegten, digital signierten Attributsdaten (Nachweis über eine Genesung

von einer Infektion mit dem bzw. eine Impfung gegen das Coronavirus SARS-CoV-2 oder ein Nachweis über einen negativen Test) durch das Auslesen mittels einer separaten und unabhängigen App, z. B. der CovPassCheck-App des RKI, beispielsweise durch einen Gastwirt erfolgt, der die ausgelesenen Daten sodann mittels Inaugenscheinnahme eines Personalausweises zu verifizieren hat,[20] initiiert im Rahmen der ID-Wallet Nutzung die zu identifizierende Person den Ausweisvorgang, indem sie mittels der ID-Wallet App einen QR-Code scannt, die ihr von der identifizierenden Person (z. B. einem Polizisten) bereitgestellt wird.

Die zu identifizierende Person besitzt keine Möglichkeit, sich Klarheit über die identifizierende Person bzw. die Stelle, für welche sie identifiziert (z. B. eine Behörde) und die Echt- und Korrektheit des QR-Codes zu verschaffen. Die initialen QR-Codes können sehr leicht hergestellt werden und in missbräuchlicher Absicht falsche Daten enthalten, [21] ohne dass hierbei Misstrauen bei der zu identifizierenden Person erweckt wird.

An dieser Stelle beginnt der Kontrollverlust, nicht nur über die in Aussicht gestellte Datensouveränität, sondern auch über die Identität selbst: Laut den Untersuchungen der IT-Sicherheitsexperten sei auf diese Weise im Rahmen der Nutzung der ID-Wallet unter bestimmten Bedingungen ein Identitätsdiebstahl möglich gewesen.[22]

Konzeptionell schwierig können die auch fehlenden Eingriffsmöglichkeiten im Hinblick auf die zu übertragenden Attribute im Gesamten und hinsichtlich der Granularität im Einzelnen sein. Wird beispielsweise in einer Verkehrskontrolle lediglich das Vorhandensein einer gültigen Fahrerlaubnis für eine bestimmte Fahrerlaubnisklasse benötigt, kann die Preisgabe eines Geburtsdatums bereits exzessiv sein. Eine Ausübung souveräner Datenhandhabung ist in der aktuellen Implementierung jedenfalls nicht vorgesehen. Es mag zudem in bestimmten Situationen wenig empfehlenswert sein, im Rahmen einer behördlichen Aufforderung ein Mobiltelefon im entsperrten Zustand weiter zu reichen.[23]

4 Souveränität im Internet

Als weitere, jedoch im Wesenskern andersartig konstruierte Werkzeuge zur Ausübung digitaler Souveränität werden seit geraumer Zeit sog. „Personal Information Management Systems" (PIMS) diskutiert. Nutzer können mit Hilfe dieser Dienste selbstbestimmt personenbezogene Daten verwalten und in die Weitergabe und Verarbeitung ihrer Daten zentral einwilligen.[24] Es handelt sich hierbei also um typische Datenintermediäre, die in der aktuellen Diskussion häufig auf den Tatbestand der Einwilligungsverwaltung beschränkt werden. Einbezogen werden allenfalls noch technische Ansätze zur Geltendmachung von Betroffenenrechten.[25] Andere Denkansätze reichen darüber weit hinaus und subsumieren auch die datentreuhänderische Verarbeitung nicht personenbezogener Daten, z. B. Daten von vernetzen Fahrzeugen, unter diesen Begriff.[26]

Auf nationaler Ebene wurden sie nicht zuletzt durch ein Gutachten der Datenethikkommission des Bundes (DEK) propagiert.[27] Solche Dienste zur Einwilligungsverwaltung kennt auch der Data Governance Act (DGA), der jedoch ebenfalls über die Idee einer Verwaltung von datenschutzrechtlichen Einwilligungen hinausgeht.[28] Der nationale Gesetzgeber hat schließlich mit dem § 26 TTDSG eine Verordnungsermächtigung für die Regulierung von PIMS geschaffen, noch bevor europaweite Regelungen zu diesen Diensten definiert wurden.[29] Inwiefern sich dieser nationale Schnellschuss als Übergangslösung oder doch als impulsgebend herausstellt, bleibt abzuwarten.

Auch bleibt abzuwarten, inwiefern tatsächlich die Gewährung von Betroffenenrechten über solche Dienste vereinfacht werden. In erster Linie könnten sie als Schutzbastion vor Tracking fungieren, vorausgesetzt, die darin hinterlegten generellen Einwilligungsversagungen würden von den Telemediendiensten befolgt. Weder aber ist momentan eine solche Befolgungspflicht zu erkennen, noch dürften PIMS, in der voraussichtlichen technischen und prozessualen Ausprägung, im Interesse irgendeines der daran Beteiligten sein. Der Datenhunger der Konzerne, die ihr Geschäftsmodell werbebasiert finanzieren, wird durch PIMS jedenfalls nicht gestillt werden. Auch mit der souveränen Entscheidung eines Endnutzers, eine Einwilligung zu versagen, wird man sich nicht zufriedengeben. Es ist zu befürchten, dass in solchen Fällen andere Methoden zur Einholung von Einwilligung „nachgeschoben" werden. Hier wird der Nutzer ähnlichen Manipulationsmustern begegnen, wie er sie bereits heute von diversen Cookie-Bannern kennt. Verantwortliche, die von solchen Mechanismen Gebrauch machen, kann man durchaus als Angreifer auf die Souveränität bezeichnen. [30] Solange dies in geschlossenen Ökosystemen stattfindet, zu deren Beitritt man nicht, weder direkt noch indirekt, verpflichtet ist, mag das Konstrukt PIMS immerhin realisierbar sein, vermutlich ohne dabei jedoch einen echten Mehrwert für den Nutzer zu bieten.

Letztlich scheitert der Gedanke an eine Datensouveränität auch an der Übermacht der Konzerngiganten. Der Ausfall von Facebook im Oktober 2021 hat gezeigt, in welchem Abhängigkeitsverhältnis die Nutzer gegenüber diesen Datenkonzernen stehen. Weitreichende Auswirkungen waren dabei nicht nur hier in Europa, sondern weltweit von enormem Ausmaß zu beobachten. Im Sinne der Datensouveränität braucht es also auch ein hohes Maß an Plattformregulierung im Hinblick auf die Sicherstellung einer Verfügbarkeit, auch jenseits der Werbemaschinerie.

20 *Löber*, Digitales EU-COVID-Zertifikat und CovPass-App: Rückkehr zur Freiheit oder Überwachungsinstrument?, ZD-Aktuell 2021, 05220, beck-online.

21 *Wittmann*, Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen, abrufbar unter https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-außer-du-musst-dich-ausweisen-829293739fa0.

22 ebenda.

23 *Neumann/Pritlove*, Logbuch Netzpolitik, Podcast-Folge 408 vom 04. Oktober 2021, LNP408 Führung in der Wurstfabrik, ab 01:44:00. Abrufbar unter: https://logbuch-netzpolitik.de/lnp408-fuehrung-in-der-wurstfabrik.

24 *Kühling*, Der datenschutzrechtliche Rahmen für Datentreuhänder, ZfDR 2021, 1.

25 *Specht-Riemenschneider/Blankertz*, Lösungsoption Datentreuhand: Datennutzbarkeit und Datenschutz zusammen denken, MMR 2021, 369.

26 *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, Die Datentreuhand, MMR-Beil. 2021, 25.

27 Das Gutachten der DEK ist abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.

28 Data Governance Act, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.

29 *Stroscher*, Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG), ZD-Aktuell 2021, 05222.

30 *Rost*, Künstliche Intelligenz trifft Datenschutz, abrufbar unter https://www.heise.de/hintergrund/Kuenstliche-Intelligenz-trifft-Datenschutz-4337027.html.

5 Die Einwilligung als Garant der Souveränität?

Es scheint dennoch, als sei die Einwilligung noch das geeignetste Mittel der Wahl zur Ausübung einer Datensouveränität, denn an sie sind strenge Anforderungen geknüpft: Sie kann ausschließlich auf freiwilliger Basis und nur für einen zuvor festgelegten, spezifischen Zweck ausdrücklich vom Betroffenen erteilt werden, nachdem er ausreichend über die konkreten Verarbeitungzwecke informiert wurde. Die Einwilligung kann darüber hinaus, dies sei im Zusammenhang mit dem souveränen Handeln besonders herausgestellt, zu einem späteren Zeitpunkt widerrufen oder gleich gänzlich versagt werden. Es mehren sich jedoch Zweifel, inwiefern dies tatsächlich als souveränes Handeln anzusehen sei. So ist alleine die Überforderung des Einwilligungsgebers bereits offensichtlich, da die Komplexität und die Menge an Einwilligungsabfragen auf Webseiten schier nicht mehr zu überblicken ist.[31] Schnell ertönt hier der Ruf nach generalisierten Einwilligungen und den bereits erwähnten PIMS. So wenig, wie die Wirksamkeit generalisiert erteilter Einwilligungen unter diesen Voraussetzungen denkbar ist, so wenig dürften es auch Einwilligungsversagungen „per default" sein, weil es in diesen Fällen stets an Konkretheit, Eindeutigkeit und Informiertheit mangelt.[32] Vermutlich haben es insofern die „do not track"-Mechanismen (DNT) bislang auch nicht in die Gesetzgebung geschafft.[33]

So verbleibt die letzte Hoffnung, Datensouveränität wenigstens über die Ausübung der übrigen Betroffenenrechte ausleben zu können. Auch hier vermag sich der Betroffene zunächst aus einem großen Werkzeugkasten von Möglichkeiten (Auskunft, Berichtigung, Löschung, Einschränkung, Übertragung) bedienen zu können, jedoch dürfte ein holistischer Ansatz auf Grund der Vielzahl an Verantwortlichen, die personenbezogene Daten verarbeiten, abschreckend wirken. Einen Überblick darüber, wie viele und welche Verantwortlichen personenbezogene Daten von ihm verarbeiten, hat der durchschnittlich versierte Internetnutzer nicht. Erschwerend hinzu kommt, dass zweifelsohne auch nach über einem halben Jahrzehnt nach dem Inkrafttreten der DSGVO noch immer nicht alle Verantwortlichen faktisch in der Lage sind, Betroffenenrechte überhaupt zu gewähren – die Gerichte sind mit solchen Fällen regelmäßig beschäftigt.[34] Es ist unverändert zu beobachten, dass dem Grundrechtsträger häufig nur dann ein Betroffenenrecht wirklich gewährt wird, wenn sich dieser mit tiefem Sachverstand, ggf. mit anwaltlicher Hilfe, an den Verantwortlichen wendet. Plattformen, um Betroffenenrechte geltend zu machen, sind noch nicht in umfangreichem Maße in Erscheinung getreten, wenngleich erste Entwicklungen vielversprechend erscheinen.

Obschon also die DSGVO betroffenenfokussiert ist, reicht dieser Arm nicht weit. Die Geltendmachung von Betroffenenrechten führt mithin, zumindest in der Praxis, auch zu keinem Souveränitätsstatus.

6 Fazit

»Das herrschende Recht ist das Recht der Herrschenden«
(Karl Marx »Zur Kritik des Gothaer Programmes«)

Der Begriff „Datensouveränität" stellt sich in der aktuellen Diskussion als eine inhaltsleere Phrase dar. In einem festen Rechtsregime kann niemand außer dem Staat souverän sein. Kein Bürger kann aufgrund der Verarbeitungspflichten und ökonomischen Zwänge Dritter frei entscheiden, welche Daten von ihm verarbeitet werden sollen. Diese Rechte und Pflichten Dritter sind nämlich unbedingt zu wahren. Souverän ist folglich allein derjenige, welcher über den Lebenszyklus einer Datenverarbeitung bestimmt – und der letztlich auch einen Datenschutzverstoß zu verantworten hat.

Datensouveränität kann nicht oder allenfalls in geschlossenen Ökosystemen existieren. Der Datengebende steht, wie ausführlich dargestellt, stets in einem enormen Abhängigkeitsverhältnis zum Datennehmenden. Der Souveränitätsbegriff darf insofern nicht missbräuchlich oder gar manipulativ verwendet werden. In Szenarien, in denen der besondere Fokus auf die Gewährung von Betroffenenrechten herausgestellt werden soll, müssen in erster Linie Taten den Worten vorangestellt sein. Wer „100% DSGVO-Konformität" oder „die volle Datenhoheit" verspricht, wird sich auch an den Details seiner technischen und organisatorischen Maßnahmen messen lassen müssen. Dazu zählt eine transparente Darlegung der Datenverarbeitung, bis in das letzte Glied der Auftragsverarbeiterkette. Dabei sollte stets auf Komplexitätsreduktion und bekannte und bewährte Technologien gesetzt werden.

Dass es eine Datensouveränität nicht geben kann, darf uns aber beruhigen: Würden jeder Mensch anstelle der Regelbefolgung seine eigene Souveränität ausleben wollen, wäre er ungeschützt vor der Souveränität der anderen.

31 *Engeler* in seinem Vortrag zum Thema „Ist die Einwilligung die Lösung oder das Problem?" auf dem Datentag der Stiftung Datenschutz, 03. Novemer 2021.

32 *Specht* in Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 9 Verbraucherdatenschutz Rn. 39.

33 *Golland*, Das Telekommunikation-Telemedien-Datenschutzgesetz, NJW 2021, 2238 Rn. 16.

34 *Suwelack*, Datenschutzrecht als neues Instrument für Massenklagen gegen Banken und Finanzdienstleister?, BKR 2021, 619.