Samstag, 29. April 2023, 15:58 Uhr
~24 Minuten Lesezeit

Lizenz zum Datenmissbrauch

Die EU will eine Datenwirtschaft etablieren und stößt damit ins gleiche Horn wie das Weltwirtschaftsforum, das uns bis 2030 jegliche Privatsphäre absprechen will.

von Simone Hörrlein
Foto: Trismegist san/Shutterstock.com

Wer eine Neuerung einführen will, die für die meisten von ihr betroffenen Menschen negative Auswirkungen

hat, der tut gut daran, die Angelegenheit so kompliziert zu machen, dass sie fast niemand mehr verstehen kann. Beim Ausbau einer totalen Überwachungsinfrastruktur muss man sich sowohl technisch als auch juristisch gut auskennen, um das Ausmaß der Bedrohung zu verstehen. Laien lassen sich von den Geschehnissen leicht überrumpeln, bis es zu spät ist. Und die Initiatoren dieses großen Staatsstreichs gegen Freiheit und Privatsphäre sind längst geübt darin, demokratische Kontrollen zu umgehen. Die Autorin erwirbt sich hier das große Verdienst, die Vorgänge und damit die Gefahr, in der wir schweben, transparent zu machen. Und sie macht Vorschläge, wie wir unsere totale Entrechtung noch abwenden können.

Bei meinen Recherchen zur elektronischen Patientenakte (ePA), die ich hier (https://www.manova.news/artikel/legalisierter-datenklau) im Rahmen eines Artikels verarbeitet habe, bin ich auf zahlreiche weitere bedenkliche Gesetze, Verordnungen und Richtlinien gestoßen, die das Gezanke um den Datenschutz und die Datenhoheit des Einzelnen gründlich ad absurdum führen. Denn in den unzähligen Verordnungen und Gesetzen, die vor unbestimmten Rechtsbegriffen nur so strotzen, geht es mitnichten um den Schutz persönlicher Daten. Das von Laien kaum durchdringbare Chaos aus Verordnungen, Paragrafenwirrwarr und unzähligen Ausnahmen verfolgt letztlich nur einen Zweck: den Datenschutz immer weiter auszuhöhlen. Ziel: der „gläserne" Bürger, der mithilfe von künstlicher Intelligenz (KI), Blockchain-Technologie, Smart Contracts und einer digitalen Zentralbankwährung (CBDC) in naher Zukunft vollautomatisiert regiert werden soll.

Auf dem europäischen Kontinent wird dieses Projekt von den demokratisch nicht legitimierten Technokraten der Europäischen Union vorangetrieben. Ihre Saat der letzten Jahrzehnte, die aus zahlreichen undemokratischen Verträgen besteht, die an den Gesetzen der Nationalstaaten vorbei verabschiedet wurden, geht nun auf, indem den einzelnen Staaten immer mehr Souveränität entzogen wird. Das Projekt Datenwirtschaft wurde aber keineswegs von den einfältigen Bürokraten der EU erdacht, sie sind lediglich die Ausführenden. Dahinter stehen einflussreiche Internationalisten, die eine Global Governance propagieren, hinter der sich nichts anderes versteckt als ein durch Algorithmen regulierter, verantwortungsloser und nicht mehr zur Rechenschaft zu ziehender Ordnungsstaat.

Persönliche Daten sollen ökonomisiert werden

Die ePA, über deren Problematik ich in obigem Artikel ausführlich berichtet hatte, ist zwar nur ein kleines, aber extrem wichtiges Teilchen in einem gigantischen Puzzle, das sich **Europäische Datenstrategie** (https://www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2021/06/europaeische-datenstrategie-062021.pdf?__blob=publicationFile) nennt. Denn erst die standardmäßige Nutzung der ePA macht den Weg frei zur Ökonomisierung selbst sensibelster medizinischer Daten. Wer sich die Mühe macht und sich in die verschiedenen Verordnungen einliest, die Grundlage der Europäische Datenstrategie und damit der geplanten Datenwirtschaft sind, versteht, weshalb kein öffentlich-rechtliches Medium dieses heiße Eisen aufgreift. Denn die dort in kryptischen Rechtstermini fein säuberlich niedergeschriebenen Veränderungen sollen nicht nur die Wirtschaft, sondern auch die gesamte Gesellschaft auf den Kopf stellen.

> ***Die unzähligen Vorschriften, mit ihren Hunderten Paragrafen und Artikeln, gaukeln dabei stets Datenschutz vor, opfern diesen aber in Wirklichkeit Schritt für Schritt wirtschaftlichen Interessen.***

Das dürfte auch der Grund sein, weshalb dieser Wust an Verordnungen und Gesetzen im öffentlichen Raum lieber totgeschwiegen und ausschließlich in akademischen Kreisen diskutiert wird.

Diese Kreise maßen sich an, über den Kopf der Bevölkerung hinweg, als wäre sie entmündigt, zu entscheiden, wie deren persönlichste Daten zu nutzen seien. Was in den Köpfen solcher Akademiker vorgeht, zeigt der **Leitartikel** (https://eizpublishing.ch/wp-content/uploads/2023/01/EuZ-digital-Holznagel-Data-Act-V1_02-20230130.pdf) in der *Zeitschrift für Europarecht* (EuZ) mit dem Titel „EU Data Act: ein wichtiger Baustein in der Europäischen Datenstrategie". Dort führen Bernd Holznagel, Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht an der Westfälischen Wilhelms-Universität Münster, und sein Doktorand Benedikt Freese nicht nur aus, wie sich das weltweite Datenvolumen entwickeln wird, sondern fabulieren auch darüber, wie sich dieser Datenschatz — womit sie auch persönlichste Daten meinen — ökonomisch und gesellschaftlich heben lässt.

Holznagel und Freese fokussieren sich in ihrem Artikel auf den **Data Act** (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113)-Vorschlag der Europäischen Kommission. Dieser sehe vor, die massenhaft in der EU vorhandenen Daten endlich effizient zu nutzen, schreiben die Autoren. Dafür seien im Verordnungsentwurf immense Reformen vorgesehen, wobei sektorübergreifende Datenzugangsansprüche für Privatpersonen und öffentliche Stellen gegen Dateninhaber — also jedes Individuum — im Fokus stünden. Weiterhin verweisen die Autoren darauf, dass der EU Data Act nur

einer von vielen wichtigen Baustein in der Europäischen Datenstrategie sei, die in nächster Zeit schrittweise umgesetzt würden.

Schauen wir uns also die verschiedenen Bausteine einmal an: Da wäre die **Open Data-Richtlinie** (https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data), die den Zugang zu Daten der öffentlichen Hand — Government-to-Business und Government-to-Consumer — regelt. Der **Data Governance Act (DGA)** (https://digital-strategy.ec.europa.eu/en/policies/data-governance-act) befasst sich mit den Vorgaben für die Weiternutzung von sensiblen Daten durch öffentliche Stellen. Besonders interessant im DGA sind Artikel 10 ff., der „Datenvermittlungsdienste" reguliert, sowie Artikel 2 Nr. 16, 16 ff., der sich mit dem Datenaltruismus, also der freiwilligen Datenspende zur gemeinsamen Datennutzung für „gemeinwohlorientierte" Zwecke beschäftigt. Weitere Informationen zum DGA finden Sie **hier** (https://www.european-data-governance-act.com/).

Damit die Datenwirtschaft bald so richtig Fahrt aufnehmen kann, hat die EU zudem den **Digital Markets Act (DMA)** (https://www.eu-digital-markets-act.com/) ins Leben gerufen, der das Funktionieren des Wettbewerbs in der Datenwirtschaft sicherstellen soll. Weitere wichtige Bausteine zur Legalisierung des geplanten Datenraubs sind der kürzlich in Kraft getretene **Digital Services Act (DSA)** (https://www.eu-digital-services-act.com/) und der **Verordnungsentwurf** (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=FR) zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

Was sich hinter der europäischen Datenstrategie, die auch von zahlreichen Machbarkeitsstudien flankiert wird, wirklich versteckt, findet man auf der Website der **Europäischen Kommission** (https://commission.europa.eu/strategy-and-policy/priorities-

2019-2024/europe-fit-digital-age/european-data-strategy_de).
Dort heißt es wörtlich:

„*Die europäische Datenstrategie soll die EU an die Spitze einer datengesteuerten Gesellschaft bringen. Ein Binnenmarkt für Daten ermöglicht eine EU-weite und branchenübergreifende Datenweitergabe zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen.*"

> ***Das Einzige, was in diesen Dokumenten und den vielen bunten Hochglanzbroschüren zur Datenwirtschaft fehlt, ist der Nutzen für die Datenlieferanten. Diese werden, wohl auch aufgrund ihrer mangelnden rechtlichen Expertise, ihrer Gutgläubigkeit und ihres Desinteresses, mit infantilen und teilweise sogar dummen Phrasen abgespeist.***

Frei nach dem Motto: Die Abgabe der Privatsphäre dient dem Gemeinwohl, damit wir endlich alle in einer besseren Welt leben können. Und während die Bürgerinnen und Bürger dazu animiert werden, ihre Daten für das Gemeinwohl zu spenden, machen andere daraus ein gigantisches Geschäftsmodell.

Ein Artikel auf der Website der Unternehmensberatung McKinsey bringt es auf den Punkt:

„*Der explosionsartige Anstieg der Nachfrage nach Rechenzentren hat die Aufmerksamkeit von Investoren aller Art auf sich gezogen (…). Allein auf dem US-Markt wird die Nachfrage — gemessen am Stromverbrauch, der die Anzahl der Server widerspiegelt, die ein Rechenzentrum beherbergen kann — laut einer McKinsey-Analyse bis 2030 voraussichtlich 35 Gigawatt (GW) erreichen, gegenüber 17 GW im Jahr 2022.*"

Besteht vielleicht eine winzige Möglichkeit, dass die steigenden

Strompreise und das Gerede von Rationierung mit dem wachsenden Strombedarf der geplanten Datenwirtschaft zu tun haben könnten?

Für das starke Wachstum des Geschäfts mit personenbezogenen Daten spricht auch die Prognose von Statista, nachdem digital-transformierte Unternehmen Ende 2023 voraussichtlich 53,3 Milliarden US-Dollar des globalen Bruttoinlandsprodukts (BIP) ausmachen werden; 2018 waren es noch **13,5 Milliarden gewesen** (https://www.statista.com/statistics/1134766/nominal-gdp-driven-by-digitally-transformed-enterprises/).

Totschlagargument „Berechtigtes Interesse"

Einer der wichtigsten Bausteine zum Abgreifen der persönlichsten Daten von Bürgern und Bürgerinnen in der EU ist die **Datenschutz-Grundverordnung (DSGVO)** (https://dsgvo-gesetz.de/), in der zahlreiche Gefahren schlummern.

> ***Bei näherer Betrachtung entpuppt sich die DSGVO eher als eine Lizenz zum Datenmissbrauch denn als eine Verordnung zum Datenschutz.***

Wie dieser Pseudodatenschutz in der Praxis aussieht, durfte ich vor einigen Tagen sogar am eigenen Leib erfahren.

Von der in den Niederlanden ansässigen Firma CompanySpotter flatterte eine E-Mail in mein Postfach. In der E-Mail wurde mir mitgeteilt, dass man meine Website, die keine Firmenseite ist, in die Suchmaschine Company Spotter aufgenommen hätte. Sämtliche personenbezogenen Daten seien in die Datenbank der Firma aufgenommen worden und würden für die Erbringung der Dienstleistungen des Unternehmens gespeichert und verarbeitet.

Die Daten würden so lange gespeichert, wie sie in der Quelle — Website — vorhanden seien, und es bestünde auch die Möglichkeit, dass sie an Empfänger innerhalb und außerhalb der EU übermittelt würden.

Als Rechtfertigung für die Speicherung meiner Daten verwies die Firma auf die DSGVO:

„Gemäß der DSGVO soll jede Verarbeitung von personenbezogenen Daten, auch die von CompanySpotter durchgeführte, gerechtfertigt sein. Die Vorschriften besagen, dass die Verarbeitung gerechtfertigt ist, wenn der Zweck der Verarbeitung auf einen der sechs in der Verordnung genannten Rechtsgründe gestützt werden kann. Die von CompanySpotter im Rahmen vom Aufbau der Datenbank vorgenommene Verarbeitung ist zur Ausübung der ‚berechtigten Interessen' von CompanySpotter und seiner Nutzer erforderlich. Es wurde bestimmt, dass die Grundrechte und Grundfreiheiten der betreffenden Person, die den Schutz personenbezogener Daten erfordern, diese berechtigten Interessen nicht überwiegen."

Den letzten Satz musste ich dreimal lesen: Es wurde also bestimmt, dass ein wie immer ausgestaltetes „berechtigtes Interesse" einer Firma über dem Schutz meiner personenbezogenen Daten steht. Damit musste ich mich erst einmal auseinandersetzen und stieß in der DSGVO tatsächlich auf den unbestimmten Rechtsbegriff des „berechtigten Interesses". Dieser Rechtsbegriff ermöglicht quasi jedem die Nutzung personenbezogener Daten, der glaubhaft machen kann, dass seine Interessen, die seiner Kunden, Nutzer und so weiter über den Grundrechten und Grundfreiheiten der betreffenden Person stehen, deren Daten genutzt werden sollen.

Berechtigtes Interesse schlägt Datenschutz

Auf der **Website** (https://keyed.de/blog/einwilligungserklaerung/) des privaten Datenschutzdienstleisters Privacy is Key(ed) GmbH gibt es ein Muster einer Einwilligungserklärung nach DSGVO 2023, in der auch das ominöse „berechtigte Interesse" aufgeführt ist. Unter Punkt sechs der Erklärung heißt es:

„Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (Artikel 6 Absatz 1 lit. f DSGVO)."

> ***Dass die „berechtigten Interessen" von Unternehmen oder Regierungen in den meisten Fällen über den Grundrechten und Grundfreiheiten der betroffenen Person stehen werden, zeigen bereits einige Urteile.***

So auch ein Urteil des Oberlandesgerichts (OLG) München, das sich mit dem nicht näher definierten „berechtigen Interesse" befasst hat. Im **Urteil** heißt es, „berechtigtes Interesse" sei weit zu interpretieren. Dies bedeute, dass die Weitergabe von Kundendaten vom europäischen Gesetzgeber also grundsätzlich vorgesehen ist. Bei der vorzunehmenden Abwägung zwischen den Interessen der Betroffenen und des Verantwortlichen beziehungsweise des Dritten sieht das Gericht eine möglichst weite Auslegung des „berechtigten Interesses" als (unions-)grundrechtlich geboten an. Nicht nur rechtliche Interessen seien dabei zu berücksichtigen, sondern auch wirtschaftliche oder ideelle.

So weit die Meinung des Gerichts, welches das „berechtigte Interesse" schon einmal über den Datenschutz der Einzelnen stellt und auch die Datennutzung eher als wünschenswert und rechtskonform ansieht.

Es wird also im Rahmen der totalen Digitalisierung darauf

hinauslaufen, dass personenbezogene Daten bald keinem Schutz mehr unterliegen und jeder Mensch aufgrund seines Profils kategorisiert und je nach Kategorie vielleicht sogar unterschiedlich behandelt werden kann.

Wird also in einer nicht mehr allzu fernen Zukunft das gesamte Leben, der Lebensstil und die bürgerlichen Freiheiten des Einzelnen, von den personenbezogenen Daten abhängig sein? Wie einfach Ungerechtigkeiten und Diskriminierungen etabliert werden können, haben die letzten drei Jahre eindrucksvoll gezeigt: Menschen, die sich auf die körperliche Unversehrtheit beriefen oder eine politisch unerwünschte Meinung hatten, wurden im Rahmen einer wahren Medienhetze diffamiert und ausgegrenzt. Kann man einer solchen Politik und einer derart verrohten Gesellschaft vertrauen? Muss man nicht vielmehr annehmen, dass man im Falle einer gegenteiligen als der veröffentlichten Meinung mit heftigsten Konsequenzen zu rechnen hätte?

Was sind personenbezogene Daten?

Wie der Rechtsbegriff „berechtigtes Interesse" ist auch der Rechtsbegriff „personenbezogene Daten" in der DSGVO weit gefasst. Die Definition von personenbezogenen Daten finden wir in Artikel 4 Nr. 1 DSGVO. Dort heißt es etwas kryptisch:

„*Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar gilt eine Person, wenn sie direkt oder auch indirekt durch eine Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen*

Person sind, identifiziert werden kann.”

Etwas genauer erläutert die Firma Privacy is Key(ed) GmbH ihren Kunden, was es mit **personenbezogenen Daten** (https://keyed.de/blog/speicherung-personenbezogener-daten/) auf sich hat.

Darunter fallen:

- Allgemeine Personendaten wie zum Beispiel Name, Geburtstag, Geburtsort, Anschrift, E-Mail-Adresse.
- Besondere Personendaten wie zum Beispiel religiöse oder politische Ansichten, Gesundheitsdaten oder genetische Daten.
- Körperliche Informationen wie zum Beispiel Geschlecht, Status, Kleidergröße, Haar- und Augenfarbe.
- Kennziffern wie zum Beispiel Sozialversicherungsnummer, Krankenversicherungsnummer und Steueridentifikationsnummer.
- Bankdaten wie zum Beispiel Kontonummer, Kontostand und weitere Informationen über die Bankverbindung wie eine IBAN.
- Onlineinformationen wie zum Beispiel IP-Adresse oder sogenannte Fingerprint-Informationen für Browser oder Geräte.
- Bewertungen wie zum Beispiel Zeugnisse oder Noten.
- Kundendaten wie zum Beispiel Bestellangaben oder Zahlungsdaten.
- Vermögensinformationen wie zum Beispiel Einkommen, Eigentum, Vermögensstand.

> ***Jeder, der ein „berechtigtes Interesse” glaubhaft machen kann, wird also künftig alles was es über einen Menschen zu wissen gibt, auch wissen können.***

Jedes Unternehmen und jede Regierung kann Ihre Vermögenswerte, Ihre Zeugnisse, Ihren Kontostand, Ihre politischen Ansichten, Ihre

Gesundheits- und sogar Ihre genetischen Daten einsehen. Und diese Daten dürfen gemäß DSGVO nicht nur gespeichert und verarbeitet, sondern auch an Dritte innerhalb und auch außerhalb der EU weitergegeben werden.

Datenklau datenschutzrechtlich optimieren

Wer sich mit dem umfangreichen Service von Privacy is Key(ed) befasst, beginnt zu begreifen, für wen die DSGVO und alle anderen „Datenschutz-Verordnungen" der EU ins Leben gerufen wurden und welchem Zweck sie tatsächlich dienen: der totalen Digitalisierung des öffentlichen und privaten Lebens, der Digitalisierung von allem und jedem. Privacy is Key(ed) beschreibt sich selbst folgendermaßen:

„*Wir optimieren Organisationen hin zu Datenschutz-Champions, sodass von enormen Wettbewerbsvorteilen, Haftungsreduktionen und gestiegener Qualität (der Daten) profitiert werden kann. Bei Keyed sind Organisationen in bester Gesellschaft. In unserem Unternehmensverbund dürfen wir bereits über 450 Organisationen jeglicher Größe datenschutzrechtlich optimieren.*"

Stärkt die DSGVO, wie das Bundesministerium der Justiz auf seiner **Website** (https://www.bmj.de/DE/Themen/FokusThemen/DSGVO/DSVGO_node.html) glaubhaft machen will, tatsächlich die Selbstbestimmung des Einzelnen über die Kontrolle seiner Daten? Um diese Frage zu beantworten, müssen wir etwas tiefer in die Verordnung einsteigen. Artikel 13 der DSGVO regelt die Informationspflicht; derjenige, der die personenbezogenen Daten erhebt und somit verarbeitet, muss den Datenlieferanten darüber informieren, welche Daten von ihm genutzt und wie sie verarbeitet

werden. Wie dies im Internet funktioniert, können wir bereits jetzt sehen: Auf so gut wie jeder Website muss der Nutzer der Verarbeitung bestimmter Daten zustimmen, will er deren Angebot nutzen. Das ist nichts anderes als Pseudoselbstbestimmung und Pseudokontrolle, denn wer nicht einwilligt, wird ausgesperrt. Das ist Nötigung, die im Falle einer Beschwerde ganz einfach mit dem Hausrecht der Anbieter gerechtfertigt wird. Es ist exakt das gleiche Muster, das wir bereits bei den Masken sahen: Das jeweilige Unternehmen entscheidet, ob es Sie ohne Maske bedient oder Ihnen den Service verweigert.

Wann ist die Speicherung personenbezogener Daten erlaubt?

Der Selbstbestimmung und Kontrolle über die eigenen Daten widerspricht auch, dass gemäß DSGVO und Bundesdatenschutzgesetz (BDSG) die Speicherung und Verarbeitung personenbezogener Daten in bestimmten Fällen sogar ohne Einwilligung möglich ist. Die Nutzung ist ohne Einwilligung rechtmäßig:

- Zur Erfüllung einer rechtlichen Verpflichtung.
- Um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Wenn die Speicherung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

> ***Auch hier haben wir das Problem der unbestimmten Rechtsbegriffe, die vielfältig ausgelegt werden können. Was sind „lebenswichtige Interessen einer anderen natürlichen Person?" Und wann liegt „öffentliches Interesse" vor? Solche unbestimmten Rechtsbegriffe***

> ***können wie ein Boomerang zurückschlagen.***

Sogar die als besonders schützenswert angesehenen besonderen personenbezogenen Daten, worunter rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung gehören, dürfen verarbeitet und gespeichert werden, sofern die in **Artikel 9 Absatz 2 DSGVO** (https://dsgvo-gesetz.de/art-9-dsgvo/) aufgeführten Ausnahmen erfüllt sind:

So dürfen Verantwortliche im Bereich Arbeits- und Sozialrecht diese Daten nutzen. Zudem dürfen sie genutzt werden, wenn der Betroffene sie bereits im Netz öffentlich gemacht hat.

Auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaates dürfen diese Daten genutzt werden, wenn die Nutzung in angemessenem Verhältnis zu dem verfolgten Ziel steht.

Auch hier die Frage: Wann steht die Nutzung derart sensibler Daten in einem angemessenen Verhältnis zum verfolgten Ziel? Wer definiert, was angemessen ist, und was, wenn der Dateninhaber dies völlig anders sieht? Bei unbestimmten Rechtsbegriffen hat Willkür schon immer Tür und Tor geöffnet.

Ein Nutzungsrecht ist zudem gegeben für die Gesundheitsvorsorge, die Arbeitsmedizin, die Beurteilung der Arbeitsfähigkeit von Beschäftigten, die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats.

Weiterhin dürfen diese Daten aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats verarbeitet werden.

Damit dürfen sogar die sensibelsten Daten der gesamten Bevölkerung quasi für fast alles genutzt werden. Dies bestätigt auch Nils Möllers, Gründer und Geschäftsführer von **Privacy is Key(ed)** (https://keyed.de/blog/besondere-personenbezogene-daten-nach-dsgvo/): „Hat man eine passende Ausnahme für die Verarbeitung besonderer personenbezogener Daten gemäß Artikel 9 Absatz 2 DSGVO gefunden, spricht prinzipiell nichts gegen die Verarbeitung von diesen Daten."

Und Möllers führt weiter aus, dass trotz des Verbotes der Speicherung hochsensibler Daten in der Cloud auch hier Umgehungsmöglichkeiten vorhanden sind: „Sehr spannend, vor allem für digitale und agile Unternehmen, ist die Frage, ob besondere personenbezogene Daten in der Cloud gespeichert werden dürfen. Das ist möglich, wenn erst mal eine Ausnahme gemäß Artikel 9 Absatz 2 DSGVO gegeben ist, (...)." Ein Datenschutzbeauftragter müsse dann nur sicherstellen, dass sich das Unternehmen nicht angreifbar für etwaige Bußgelder oder Schadensersatzforderungen macht, so Möllers.

Wohin diese Datenwirtschaft final führen soll und wird, zeigt § 31 Bundesdatenschutzgesetz, wonach personenbezogene Daten auch für Scoring und Bonitätsauskünfte verwendet werden dürfen. Und es wird noch besser: Auch Wahrscheinlichkeitswerte über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person wären

rechtmäßig.

Das ist nicht mehr weit entfernt von der Dystopie des Hollywood-Streifens „Minority Report". Heute wird Ihnen vielleicht nur ein Kaufvertrag verwehrt, morgen werden Sie dann möglicherweise prophylaktisch aus dem Verkehr gezogen, denn Sie hätten übermorgen ganz sicher eine Straftat begangen. Wie wir ja alle wissen, KI irrt nie, sie ist unfehlbar. Es geht in § 31 darum, dass intelligente Algorithmen auf Basis aller gesammelten Daten einer Person prognostizieren, wie sich diese Person in der Zukunft verhalten wird. Dies nennt man gemeinhin Profiling, und das kam bisher lediglich in der Kriminalistik zum Einsatz. Einen passenden Artikel dazu findet man auch in der DSGVO: Artikel 22 Automatisierte Entscheidungen im Einzelfall einschließlich **Profiling** (https://dsgvo-gesetz.de/art-22-dsgvo/).

Sehen wir uns diesen Artikel einmal etwas genauer an. In Absatz 2 liest man, dass Profiling erlaubt ist:

1.Wenn es für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist.
2. Wenn es aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten.
3. Wenn eine ausdrückliche Einwilligung der betroffenen Person vorliegt.

Und selbst die besonderen personenbezogenen Daten sind in diesem Falle nicht tabu, sofern **Artikel 9 Absatz 2 Buchstabe a oder g** (https://dsgvo-gesetz.de/art-9-dsgvo/) gilt. Buchstabe a regelt die freiwillige Zustimmung, Buchstabe g ermöglicht die Verarbeitung auf der Grundlage des Unionsrechts oder des Rechts

eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, beziehungsweise aus Gründen eines erheblichen öffentlichen Interesses.

Es wird in der neuen Datenwirtschaft sehr wahrscheinlich darauf hinauslaufen, dass personenbezogene Daten nur noch in Ausnahmefällen einem Schutz unterliegen. Schließlich sind Daten die Währung dieser Wirtschaft — ohne Daten keine Datenwirtschaft. Dass Menschen aufgrund ihres Profils kategorisiert und je nach Kategorie unterschiedlich behandelt werden, dürfte dann nicht die Ausnahme, sondern die Regel sein.

Wie könnte so eine auf Profiling und Verhaltensvorhersage basierende Wirtschaft aus dem Ruder laufen? Könnten einer Person im Falle von unkorrektem Verhalten, einer unerwünschten politischen Meinung, der falschen Wohngegend, zu wenig Geld auf dem Konto, des falschen Geschlechts, der falschen Hautfarbe oder der falschen sexuellen Orientierung ein Job oder bestimmte Services und Dienstleistungen verweigert werden? Das ergibt einen Sinn, weil es zur Identitätspolitik passt, die immer mehr um sich greift und Menschen aufgrund ihrer persönlichen Merkmale in Gruppen einteilt, um sie unterschiedlich zu behandeln. Offiziell heißt es, dies diene der Verhinderung von Diskriminierung. Nein, das *ist* Diskriminierung!

Der „Verordnungsvorschlag für die Festlegung harmonisierter Vorschriften für künstliche Intelligenz" zeigt, dass die Nutzung von KI wahrscheinlich in eine Art Zentralstaat mit zentraler Ressourcenverteilung führen wird:

„*Der Einsatz künstlicher Intelligenz zur Verbesserung von Prognosen, zur Optimierung von Abläufen und der Ressourcenzuweisung sowie zur Personalisierung der Diensteerbringung kann für die Gesellschaft und die Umwelt von Nutzen sein und Unternehmen sowie der europäischen Wirtschaft Wettbewerbsvorteile verschaffen. Bedarf*

besteht insbesondere in Sektoren, von denen eine große Wirkung ausgeht, wie Klimaschutz, Umwelt und Gesundheit, öffentlicher Sektor, Finanzen, Mobilität, Inneres und Landwirtschaft."

Individuelle Kategorisierung, Profiling und Verhaltensvorhersage zeichnen, zusammen mit KI, auf Blockchain-Technologie basierenden Smart Contracts sowie einer **digitalen Währung (CBDC)** (https://www.ledgerinsights.com/digital-euro-legislation-cbdc/), ein ziemlich düsteres Bild. Denn wer kein Bargeld mehr besitzt, der besitzt — in einem von KI gesteuerten vollautomatisierten Ordnungsstaat, der das Leben bis in kleinste Detail regelt — auch nicht mehr die Freiheit, das zu tun, was er möchte. In einem Staat, in dem KI die Deutungshoheit erhält und niemand mehr zur Rechenschaft gezogen werden kann, werden Beschwerden ins Leere laufen und Rechtsstreite werden obsolet.

CBDC, eine kryptofaschistische Währung

Dass die Zentralbankwährung CBDC kommen wird, ist keine Frage. Die Frage ist nur, wann sie kommen wird und wie sie ausgestaltet sein wird. Die EU-Kommission will noch in 2023 eine entsprechende Verordnung dazu zu erlassen; die Einführung der CBDC ist dann zwischen 2026 und 2027 geplant. Laut einer **Presseerklärung** (https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews220916.en.html) vom 16. September 2022 evaluiert die Europäische Zentralbank (EZB) gerade mit fünf Partnern die technische Machbarkeit einer CBDC; neben zahlreichen Banken ist auch der Tech-Konzern Amazon mit an Bord.

Über die Ausgestaltung der CBDC haben sich die Damen und Herren der EZB schon einige Gedanken gemacht. Fabio Panetta, Mitglied des EZB-Direktoriums, stellte in einem **Interview**

(https://www.ecb.europa.eu/press/inter/date/2021/html/ecb.in210620%7Ec8acf4bc2b.en.html) mit der *Financial Times* der Öffentlichkeit schon einmal sein ganz persönliches „Brainchild" vor: Für den digitalen Euro sieht er eine Obergrenze von maximal 3.000 Euro, er kann sich zwar auch höhere Beträge vorstellen, die Betroffenen müssten dann aber finanziell benachteiligt werden. Diese Benachteiligung könnten Strafzinsen oder auch ein Verfallsdatum sein. Auch China denkt über diesen Raubzug mittels Verfallsdatum bereits öffentlich nach, und China könnte, wenn es nach Klaus Schwab geht, ein Vorbild für viele Länder werden. Sparen — für einen Urlaub, ein Auto oder was man sich sonst noch so wünscht — wäre dann ein für allemal Vergangenheit. Der Spruch „Leben von der Hand in den Mund" würde damit eine ganz neue Bedeutung erlangen.

Ich schließe mich bei meiner Bewertung der CBDC dem amerikanischen Whistleblower und Sicherheitsexperten Edward Snowden an. Snowden schreibt auf seinem **Blog** (https://edwardsnowden.substack.com/p/cbdcs): Diese CBDCs sind keine Innovation, sondern „kryptofaschistische Währungen", die dem Zweck dienen, ihren Nutzern „das grundlegende Eigentum an ihrem Geld zu verweigern und den Staat als Vermittler jeder Transaktion einzusetzen".

> ***Hinzu kommt, dass dieses Pseudogeld aus Bits und Bytes, das noch weniger Wert als unser gegenwärtiges Fiat-Money besitzt, zur totalen Kontrolle der Gesellschaft genutzt werden soll und zur totalen Abhängigkeit von einer nicht legitimierten supranationalen Organisation führen wird.***

Spürbar dürfte diese Abhängigkeit spätestens dann werden, wenn KI — wie geplant — immer mehr Arbeitsplätze vernichten wird. Dass totale Kontrolle ein primäres Ziel ist, bestätigt auch Agustín Carstens, seines Zeichens Generaldirektor der Bank für

Internationalen Zahlungsausgleich (BIZ). Während einer Podiumsdiskussion des Internationalen Währungsfonds (IWF) im Jahr 2020 sagte Carstens:

„Wir wissen nicht, wer heute einen 100-Dollar-Schein benutzt, und wir wissen nicht, wer heute einen 1.000-Peso-Schein benutzt. Der Hauptunterschied einer CBDC besteht darin, dass die Zentralbank die absolute Kontrolle über die Regeln und Vorschriften hat.“

Digitale Identität und Wallet bald verpflichtend

Damit eine Datenwirtschaft funktioniert, braucht es aber nicht nur digitales Geld, sondern auch die Möglichkeit, alle persönlichen Daten eine Individuums an einer zentralen Stelle zu speichern und den Besitzer dieser Daten einwandfrei zu identifizieren. Deshalb ist es unabdingbar, dass neben der CBDC auch eine digitale ID und eine Wallet, möglichst in Form einer App, eingeführt werden. Die Europäische Kommission hat dies bereits antizipiert und lässt gegenwärtig durch das **Potenzial-Konsortium** neue Prototypen der geplanten „EU Digital Identity Wallet“ in sechs Anwendungsfällen testen: elektronische Behördendienste, Kontoeröffnung, SIM-Registrierung, mobiler Führerschein, digitale Unterschrift und elektronisches Rezept.

Laut **Haufe Online** (https://www.haufe.de/compliance/recht-politik/euid-wallet_230132_587680.html) hat der EU-Rat im Dezember 2022 auch den Änderungen der Verordnung über elektronische Identifizierung und elektronische Transaktionen im **Binnenmarkt (eIDAS-Verordnung)** (https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0281) aus dem Jahr 2014 zugestimmt. Damit steht der Einführung der sogenannten EUid-Wallet, die auch den

Rahmen für eine europäische digitale Identität schafft, nichts mehr im Wege. Gemäß der eIDAS („Electronic IDentification, Authentication and Trust Services“)-2.0-Verordnung müssen ab dem 1. Januar 2023 alle EU-Mitgliedstaaten innerhalb von maximal zwölf Monaten, also ab 2024, ihren Bürgern eine solche digitale Brieftasche zur Verfügung stellen.

Gleichzeitig soll die App als Sammelordner für digitale Dokumente aller Art dienen. Laut Verordnung ist eine Mindestliste von Attributen vorgesehen: Adresse, Alter, Geschlecht, Personenstand, Familienzusammensetzung, Staatsangehörigkeit, Bildungsabschlüsse, Titel und Erlaubnisse, Berufsqualifikationen, Titel und Berechtigungen, behördliche Genehmigungen und Lizenzen, Finanz- und Unternehmensdaten. Die App kann aber auch Ausweise, Gesundheitskarten, Zeugnisse, Eintritts- oder Mitgliedskarten aufnehmen und bereitstellen.
Besonders „datenschutzfreundlich”: Die überarbeitete Version der Verordnung sieht vor, dass nicht mehr nur Behörden, sondern auch private Unternehmen die Dokumente in der Wallet nutzen können. Und damit sich auch niemand der European Digital Identity Wallet entziehen kann, soll die Wallet-Nutzung in bestimmten Sektoren sogar zur Pflicht werden: Große Internetplattformen wie Google, Amazon, Facebook und eBay, aber auch Banken und Versicherungen sollen verpflichtet werden, die Wallet zu unterstützen.

Damit wird quasi jeder gezwungen, die digitale Wallet auf sein Smartphone zu laden und zu nutzen, sofern er Teil dieses Systems bleiben will oder muss. Laut **Website** (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de#vorteile-der-europ%C3%A4ischen-digitalen-identit%C3%A4t) der Europäischen Kommission sollen ID und Wallet künftig auch für folgende Dinge genutzt werden:

- Nutzung aller öffentlichen Dienste zum Beispiel zur Beantragung von Geburtsurkunden und ärztlichen Attesten oder zur Mitteilung von Adressänderungen.
- Eröffnung eines Bankkontos.
- Steuererklärung.
- Bewerbung an einer Hochschule innerhalb der EU.
- Speicherung eines ärztlichen Rezepts, das überall in Europa eingelöst werden kann.
- Altersnachweis.
- Anmietung eines Autos mit digitalem Führerschein.
- Check-in in einem Hotel.

Datenschutzbeauftragte schlagen Alarm

Die Änderung der eIDAS-Verordnung ist ein digitaler Albtraum. Sogar der Bundesdatenschutzbeauftragte, Professor Ulrich Kleber, warnt in obigem Artikel bei Haufe Online davor, dass mit dieser Verordnung nicht nur ein zentraler Datenklau, sondern auch ein profilübergreifendes Tracking drohe. Womit er meine Bedenken und meine Kritik an dieser Verordnungswut untermauert. Zudem, warnt Kleber, würden dort Informationen aus zahlreichen Lebensbereichen zusammengeführt, die die gesamte EU-Bevölkerung „gläsern“ machten. Tja, wär hätte das gedacht? Hinzu käme, dass auch der Datenschutz nicht gewährleistet sei, da beim Datentransfer mit QWACs (Qualified Website Authentication Certificates, Qualifizierte Zertifikate für die Website-Authentifizierung) veraltete und unsichere Sicherheitszertifikate eingesetzt werden sollen. Erklärtes Ziel der EU sei es, dass 2030 80 Prozent aller Bürgerinnen und Bürger die EUid-Wallet nutzen. Das passt perfekt zu den Zahlen der ePA, die man ebenfalls mindestens

80 Prozent der Menschen in Deutschland aufs Auge drücken möchte.

Auch der Landesdatenschutzbeauftragte Bayerns, Thomas Petri, den ich mit meinen Bedenken zur ePA und zum Europäische Gesundheitsdatenraum (EHDS) konfrontiert hatte, teilt meine zahllosen Bedenken. In seiner Antwort-E-Mail schreibt er:

"*Die Gesetzesinitiative der Europäischen Kommission zur Verordnung über einen gemeinsamen europäischen Gesundheitsdatenraum (European Health Data Space, - EHDS) sehe ich wie Sie sehr kritisch.*"

Petri bestätigt auch meine Bedenken, dass der EHDS nicht nur die Primärdatennutzung, also die Verarbeitung von Gesundheitsdaten im Rahmen von Gesundheitsdienstleistungen, regeln will, sondern dass es auf die Abschaffung des deutschen Patientengeheimnisses hinausläuft.

Zudem sieht auch Petri die Sekundärdatennutzung, also die Nutzung von elektronischen Gesundheitsdaten, unter anderem zur wissenschaftlichen Forschung, zu Fortbildungszwecken oder zur Weiterentwicklung von medizinischen Produkten und Dienstleistungen, genauso kritisch, wie ich das tue. Laut Petri sollen Dateninhaber — also die gesamte EU-Bevölkerung — nach den Vorstellungen der Europäischen Kommission sogar dazu verpflichtet werden, auf Anforderung von „berechtigten" Antragstellern, die von ihnen verarbeiteten elektronischen Gesundheitsdaten zur Verfügung zu stellen. Der Verordnungsvorschlag der Europäischen Kommission sähe dabei nicht vor, dass die betroffenen Personen diese Verpflichtung in irgendeiner Weise unterbinden können. Es seien vielmehr überhaupt keine Partizipationsrechte hinsichtlich des „Ob" der Sekundärnutzung der persönlichen elektronischen Gesundheitsdaten vorgesehen.

Wir dürfen nicht tatenlos zusehen!

Was schon seit ziemlich langer Zeit hinter dem Rücken der Bevölkerung und ohne jede demokratische Mitbestimmung von ein paar nicht demokratisch legitimierten Technokraten abgezogen wird, nenne ich einen handfesten Skandal. Im Hinblick auf die bereits umfangreiche Gesetzeslage, die von der Europäischen Kommission klammheimlich in die Wege geleitet wurde, dürfen wir als Betroffene nicht tatenlos zusehen. Wenn wir nicht wollen, dass uns das Recht an unseren Daten bald vollständig abgesprochen wird, müssen wir handeln — alle und sofort. Datenschutzbeauftragte werden mit unseren Steuergeldern bezahlt und sind dazu da, unsere persönlichen Daten vor Missbrauch zu schützen, und wir sollten diesen Schutz schnellstmöglich einfordern.

Petri hat mir gegenüber glaubhaft gemacht, dass er sich dafür einsetzen will, aber dazu braucht er Unterstützung, also möglichst viele Menschen wie mich, die ihn anschreiben und ihren Unmut kundtun. Ich fordere deshalb alle Menschen, die am Schutz ihrer persönlichen Daten, ihrer Privatsphäre, ihrer Freiheit und der Freiheit ihrer Kinder auch nur einen Funken Interesse haben, dazu auf, sich jetzt lautstark Gehör zu verschaffen. Schreiben Sie an Ihren Datenschutzbeauftragten und fordern Sie ihn auf, seine Pflicht zu tun — nämlich Ihre Daten vor dem Zugriff Unbefugter zu schützen.

Wir müssen darauf dringen, dass unsere Daten nicht von einer Datenwirtschaft missbraucht werden, die damit Billionen von Gewinnen abschöpfen will, ohne dafür einen einzigen Cent zu bezahlen. Hinzu kommt, die Bürgerinnen und Bürger der EU sollen nicht nur ihrer Daten beraubt werden, sie sollen mit ihren Steuergeldern auch noch für diese gesamte digitale Umgestaltung zu einer Datenindustrie bezahlen.

> ***Wollen wir nicht in der Dystopie der dänischen***

> ***Politikerin Ida Auken enden, die uns bis 2030 kein Eigentum und keine Privatsphäre prognostiziert, dann müssen wir die undemokratischen Vorstöße der EU und ihrer Handlanger in der nationalen Politik, die unsere Wirtschaft in eine Datenwirtschaft transferieren wollen, gemeinsam stoppen.***

Simone Hörrlein ist Lebensmittelchemikerin und Wissenschaftsjournalistin. Nach ihrem Studium an der **TU München** war sie mehrere Jahre in der medizinischen Forschung tätig und arbeitete zuletzt in der Wissenschaftskommunikation des **Kompetenzzentrums für Ernährung**. Neben den Naturwissenschaften interessiert sie sich für Finanz- und Geopolitik. Aktuell lebt sie in Kanada.