# Das Recht der digitalen Transformation[1]

*Margrit Seckelmann*

## I. „Die Verwandlung“: Zur Einleitung

Transformare bedeutet „verwandeln“. Aber seit Franz Kafkas berühmter Novelle wissen wir, dass Verwandlungen nicht immer zum Besseren erfolgen. Wenn also nachfolgend der Begriff der „digitalen Transformation“ analysiert werden soll, so ist dieses ein risikogeneigtes Unternehmen. Es dürfte sich trotzdem lohnen, einen Versuch zu unternehmen, eine Entwicklung rechtlich zu fassen, die sich vor unser aller Augen abspielt.

Laut Wikipedia handelt es sich bei einer digitalen Transformation um „einen fortlaufenden, tiefgreifenden Veränderungsprozess in Wirtschaft und Gesellschaft, der durch die Entstehung immer leistungsfähigerer digitaler Techniken und Technologien ausgelöst worden ist“.[2] Aber was bedeutet dieses eher auf die Wirtschaft bezogene Modell eigentlich für den Staat und seine Verwaltung? Sicherlich mehr als nur das erneute Polieren der Faxgeräte und die Einrichtung eines parallelen E-Mail-Zugangs zur Verwaltung.[3] Bei den derzeit laufenden Debatten zwischen dem Deutschen Bundestag und dem Bundesrat um die Fortentwicklung des Onlinezugangsgesetzes[4] wird genau das verhandelt: Wie bekommt man den „Staat an den

1 Der Aufsatz befindet sich auf dem Stand vom 29.2.2024 und enthält eine aktualisierte Version der Antrittsvorlesung der Verfasserin am 13.7.2022. Diejenigen Passagen, die sich auf Rechtsakte (damals: Entwürfe) der Europäischen Union bzw. auf das Onlinezugangsgesetz beziehen, wurden auf den Stand am 29.2.2024 angepasst. Eine längere Version dieses Beitrags erscheint in der Zeitschrift DER STAAT (2025).

2 https://de.wikipedia.org/wiki/Digitale_Transformation (zuletzt abgerufen am 29.2.2024).

3 Vgl. dazu *Mehde*, „Corona“ als verwaltungspolitisches Argument, in: Seckelmann/ders. (Hrsg.), Der öffentliche Dienst „nach Corona“ – Beiträge zum Festkolloquium für Hans Peter Bull am 25. März 2022 an der Universität Hamburg, Tübingen 2023, S. 1-38.

4 Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG), BT-Drs. 20/8093; vom Deutschen Bundestag angenommen am 23.2.2024; die Zustimmung des Bundesrats steht im Zeitpunkt der Drucklegung noch aus.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Draht“[5] und wie sehr muss sich der Staat selbst dabei verändern (vor allem bezogen auf die Aufbau- und Ablauforganisation)?

Der Prognose nach dürfte es nicht bei einer oberflächlichen Veränderung bleiben. In der Sprache der Verwaltungsinformatik ausgedrückt, ist nicht nur das „Front Office“, sondern auch das „Back Office“ betroffen. Und mehr noch: Auch die Kompetenzverteilung des Grundgesetzes und sogar die Beziehungen zwischen der Europäischen Union und ihren Mitgliedstaaten werden von der digitalen Transformation in Frage gestellt. Denn die Digitalisierung ist ein Prozess, dem spezifische Tendenzen und Gesetzlichkeiten inhärent sind: Er folgt einer eigenen Logik, umfasst fast alle Lebensbereiche und hat deshalb natürlich auch Auswirkungen auf gesamtgesellschaftliche Strukturen.

Handelt es sich also um eine Revolution, wie wir sie beispielsweise aus der Industriellen Revolution des 19. und frühen 20. Jahrhunderts[6] kennen? Ja und nein. Der Transformationsbegriff ist komplexer. In der jüngeren Geschichtswissenschaft wird er für *Umbruchsituationen* gebraucht, „jenseits der Dichotomie von Revolution und Reaktion als komplexes Geflecht von allmählichen Veränderungen, revolutionären Episoden, adaptiven Situationen und erneuten Aufbrüchen“ und in Wechselbeziehungen „von europäischer und außereuropäischer Welt“ – in Transformationsphasen ändern sich „Strukturen, Ordnungen und Erfahrungen […] ebenso wie die Selbstdeutungen der Gesellschaft“.[7]

## II. Souveränität im digitalen Raum

### 1. Begriffsklärungen

Um eine solche Selbstdeutung des deutschen Staates in seiner Eingebundenheit in das europäische Mehrebenensystem und in seiner Abgrenzung nach außen, also zu außereuropäischen Staaten und zu außereuropäischen Wirtschaftsunternehmen, soll es nachfolgend gehen. Dieses soll insbeson-

5 Formulierung nach *Lenk*, Der Staat am Draht: Electronic Government und die Zukunft der öffentlichen Verwaltung – eine Einführung, Berlin 2004.

6 Vgl. *Vec*, Recht und Normierung in der Industriellen Revolution: Neue Strukturen der Normsetzung in Völkerrecht, staatlicher Gesetzgebung und gesellschaftlicher Selbstnormierung, Frankfurt a.M. 2006 sowie die weiteren Bände der Reihe „Recht in der Industriellen Revolution“.

7 *Planert*, Profil: Transformationen, unter: https://neuere-geschichte.phil-fak.uni-koeln.de/profil/transformationen (zuletzt abgefragt am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

dere anhand eines Begriffs dargestellt werden, der auf europäischer Ebene entwickelt wurde und der derzeit intensiv diskutiert wird. Gemeint ist die „digitale Souveränität".

Dieser Begriff ist zunächst von anderen Souveränitätsbegriffen abgrenzen. Seit einem seiner Väter, dem französischen Juristen Jean Bodin, der aus dem mittellateinischen Wort „*superanus*" das Wort „*souveraineté*" formte, bezeichnet dieser Begriff die rechtliche und faktische Möglichkeit zur Selbstbestimmung.[8] Damit kann eine Autonomie des Staates gegenüber anderen Instanzen wie der Kirche einhergehen, aber auch gegenüber Mittlerinstitutionen wie Bankhäusern oder den sogenannten Condottiere, die gegen Geld für die *Signoria* oberitalienischer Städte in den Krieg zogen.

Die Möglichkeit zur Selbstbestimmung ist auch das zentrale Moment bei dem derzeit viel diskutierten Konzept einer *self-sovereign identity*.[9] Hierbei handelt es sich allerdings um eine bestimmte Form des Rechts- und Zugangsmanagements, mit dessen Hilfe sich der oder die Einzelne ausweisen oder anderweitig legitimieren kann (und auf die später noch einmal eingegangen werden soll).

Der Begriff der „digitalen Souveränität" kennzeichnet zunächst einmal eine Grenze nach außen. Denn die Ausflaggung eines zu verteidigenden Rechts auf „digitale Souveränität" ist nämlich auch und zunächst einmal eine Kampfansage. Diese gilt neuen Akteuren wie den sogenannten Gatekeepern, namentlich dem Meta-Konzern, dem Mutterunternehmen von Facebook und Instagram. Um einen Bericht aus der Süddeutschen Zeitung zu zitieren, haben Metas Plattformen „mehr Nutzer als Länder Einwohner, die Einnahmen des Konzerns übersteigen das Bruttoinlandsprodukt mancher Volkswirtschaften. Auch die Rechtsprechung liegt größtenteils in Metas Hand, mit dem *Oversight Board* gibt es sogar eine Art Verfassungsgericht".[10] Und mit der Währung Diem (vormals Libra), die Meta ausgeben wollte, wäre sein Gründer, *Mark Zuckerberg*, sogar zum Notenbanker und Meta (so erneut die Süddeutsche Zeitung) „endgültig zum Staat" gewor-

8 *Bodin*, Les Six Livres de la République, 1576; hier zitiert nach der deutschen Übersetzung von *Niedhart*, Jean Bodin: Über den Staat, Stuttgart 2005, S. 8.

9 Vgl. dazu nur *Bundesamt für Sicherheit in der Informationstechnik*, Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT), Bonn 2021.

10 *Hurtz/Zydra*, Zuckerberg wird doch kein Notenbanker, Süddeutsche Zeitung Online v. 26.1.2022, https://www.sueddeutsche.de/wirtschaft/facebook-meta-libra-diem-ezb-waehrung-l.5515854 (zuletzt abgerufen am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

den.[11] Chinesische Unternehmen wie TikTok schicken sich an, die Verfolgung von Meta aufzunehmen, sind allerdings deutlich enger mit der chinesischen Staatsführung verbunden als Meta mit der US-amerikanischen.

## 2. Spezifika des „digitalen Raums"

Wie zieht man eigentlich die Grenze zu einem staatsähnlichen Konzern wie Meta, der sozusagen eine doppelte Staatsbürgerschaft anbietet, nämlich eine digitale zusätzlich zu einer terrestrischen, ohne dass es diesbezüglich ein Anerkennungsabkommen gäbe? So leicht die „Größen" also zu identifizieren sind, gegen die die digitale Souveränität eingeklagt und durchgesetzt werden soll, so schwierig sind sie, jedenfalls mit dem klassischen staatsrechtlichen Instrumentarium, zu verorten. Das heißt auch: Der „digitale Raum" ist anders beschaffen als derjenige klassischer Staatlichkeit – und muss erst einmal „vermessen" werden.[12] Trotzdem gibt es strukturelle Ähnlichkeiten. Denn ähnlich wie früher die Kolonialmächte konnte der Metakonzern bzw. konnten seine Vorläufer lange Zeit die Fähnchen einrammen und uns – quasi als die Eingeborenen (oder *natives*) – mit Glasperlen wie netten Internet-Gadges abspeisen, für die wir bereitwillig Kostbares (wie unsere persönlichen Daten) hergaben, von dem wir in dem Moment nur noch nicht wussten, wie kostbar es im „digitalen Kapitalismus"[13] sein wird.

Dass die Europäische Union und ihre Mitgliedstaaten hier nicht länger tatenlos zusehen wollen, liegt auf der Hand. Die Begriffsprägung der „digitalen Souveränität", die dem GAIA X-Programm der EU entstammt,[14] deutet schon an, worum es geht: um den Rückgewinn von Handlungsfähig-

11 *Hurtz/Zydra*, Zuckerberg (Fn. 10).

12 *von Lewinski*, Rechte und Rechtspositionen an und in virtuellen Räumen – Recht der Adress- und Namensräume, in: Hill/Schliesky (Hrsg.), Die Vermessung des virtuellen Raums: E-Volution des Rechts- und Verwaltungssystems III, Baden-Baden 2012, S. 177-192.

13 Vgl. zur Einführung in diesen Begriff *Staab*, Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit, Berlin 2019 sowie die Beiträge in: Carstensen/Schaupp/Sevignani (Hrsg.), Theorien des digitalen Kapitalismus: Arbeit und Ökonomie, Politik und Subjekt, Berlin 2023 (alles natürlich unter Bezugnahme auf *Zuboff*, The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power, London 2018).

14 „Ziel ist ein sicheres föderiertes Datenökosystem, das für digitale Souveränität der Dateninhaber, Interoperabilität sowie den Open-Source Gedanken steht und die föderale Idee Europas umsetzt.", https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html; vgl. auch die Darstellung auf https://gaia-x.eu/ (beides zuletzt abgerufen am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

keiten – oder zumindest um die Schaffung von Voraussetzungen eines integrativen *Electronic Government* im Sinne einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur für Europa. Das aber setzt voraus, dass die entscheidenden Kommunikationskanäle nicht oder nicht ausschließlich in den Händen Dritter liegen, sei es anderer Staaten oder sei es in den Händen von Privaten, auf die die EU und ihre Mitgliedstaaten keinen Einfluss nehmen können.

## 3. Die Entstehung einer „Europäischen Digitalverfassung"

Worin besteht eigentlich das Problem? So könnte man fragen. Die Antwort ist einfach: Diese Prinzipien müssen, so die These, heute nicht mehr nur Staaten gegenüber verteidigt werden (dieses aber natürlich auch, das hat uns der Angriffskrieg Russlands auf die Ukraine gezeigt). Die neuartige Dimension ist vielmehr die *faktische* Abhängigkeit von denjenigen, die die neuen Kommunikationsforen anbieten, den sogenannten Gatekeepern, wie es in der Diktion der Europäischen Union heißt. Dieser Kommunikationsforen in Form der sozialen Medien bedient sich seit einigen Jahren auch der Staat, zumindest in informierender Form.[15] Wenn jedoch die Staat-Bürger-Kommunikation *de facto* auf diese privaten Türhüter angewiesen ist, so muss dafür gesorgt werden, dass die entsprechenden Türen auch offenbleiben – zur Not sogar gegen den Willen der Türhüter selbst. Das Problem ist also die Existenz – und weitere Zunahme – von *privater Macht*, die fast schon Staatsqualität annehmen kann.[16]

### a) Quasi-staatliche Bindungen privater Akteure?

Das Bundesverfassungsgericht hat diese Gefahren erkannt und ist diese – für den Geltungsbereich des Grundgesetzes – auch angegangen. Seine Judi-

15 Dazu *Mast*, Staatsinformationsqualität: De- und Rekonstruktion des verfassungsgerichtlichen Leitbilds öffentlicher staatlicher Informationstätigkeit und der entsprechenden Gebote, Berlin 2020; *Seckelmann*, Einsatz bei der Polizei: Kommunikation, Online-Streifen, Trojaner, Facebook-Fahndung, Biometriesoftware, (intelligente) Videoüberwachung, Predictive Policing, Body-Cams und Fotodrohnen, in: dies. (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 3. Aufl., Berlin 2024, S. 591-621.

16 *Seckelmann*, Verwaltungshandeln in sozialen Netzwerken, in: Hill/Mehde (Hrsg.), Herausforderungen für das Verwaltungsrecht, Berlin 2023, S. 203-215.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

katur zu einer quasi-staatlichen bzw. unmittelbaren Grundrechtsbindung Privater, die es in seinen Entscheidungen zu Fraport,[17] dem Bierdosen-Flashmob[18] und dem Stadionverbot[19] sowie im Beschluss zum Eilantrag der Partei „Der Dritte Weg"[20] entfaltet hat, zeigt das.[21]

Indem das Gericht die Frage der Grundrechtsbindung an die Eröffnung grundrechtsrelevanter Räume gekoppelt hat, hat es den springenden Punkt benannt: Wer öffentliche Räume schafft und die Bedingungen freiheitlicher Kommunikation darin regulieren kann, kann sich nicht durch eine bloße Berufung auf ein *reales oder digitales Hausrecht* der Frage entziehen, unter welchen Voraussetzungen Kommunikation möglich sein soll oder eben nicht.[22]

Ob das alles rechtsdogmatisch im deutschen Recht[23] so einfach zu haben ist, sei einmal dahingestellt. Die Tendenz dazu, die Grundrechte fast oder gänzlich unmittelbar auch zwischen Privaten gelten zu lassen, wird uns immer mehr mit der Frage konfrontieren, ob die liberale Trennung zwischen Staat und Gesellschaft, wie sie unserem Grundgesetz zugrunde liegt, nicht schleichend ausgehebelt wird.[24] Und was bedeutet das eigentlich für die

17 BVerfG vom 22.2.2011, BVerfGE 128, 226.

18 BVerfG vom 18.7.2015, NJW 2015, 2485.

19 BVerfG vom 11.4.2018, BVerfGE 148, 267.

20 BVerfG vom 22.5.2019, NJW 2019, 1935.

21 Wobei außer Betracht bleiben soll, wie genau das Bundesverfassungsgericht in diesen Fällen eine quasi-staatliche Bindung Privater herleitet, vgl. dazu nur *Hellgardt*, Wer hat Angst vor der unmittelbaren Drittwirkung?, JZ 2018, 901-910; *Michl*, Situativ staatsgleiche Grundrechtsbindung privater Akteure, JZ 2018, 910-918; *Schröder*, Drittwirkung der Grundrechte – von Lüth zu Facebook, in: Knauff/Lee (Hrsg.), Verfassungsrecht und Verfassungsgerichtsbarkeit als Impulsgeber für die Rechtsentwicklung, Stuttgart 2023, S. 57-70.

22 Dazu *Ferrau*, Eine Kommunikationsordnung für Soziale Netzwerke – Zur mittelbaren Drittwirkung von Grundrechten gemäß den Facebook-Entscheidungen des Bundesgerichtshofs, Verfassungsblog v. 4.8.2021, https://verfassungsblog.de/bgh-drittwirkung-fb/; vgl. auch *Friehe*, Soziale Netzwerke in der Grundrechts-Klemme?, Verfassungsblog v. 7.5.2021, https://verfassungsblog.de/soc-med-klemme/ (beides zuletzt abgerufen am 29.2.2024).

23 Zur Europäischen Menschenrechtskonvention und zur Europäischen Grundrechte-Charta vgl. *Gusy*, Grundrechtsbindungen Privater, Jus Politicum Nr. 10 (März 2014), online: https://juspoliticum.com/article/Grundrechtsbindungen-Privater-735.html (zuletzt abgerufen am 29.2.2024).

24 Umgekehrt hat *Kulick* in seiner 2020 veröffentlichten Habilitationsschrift ein Plädoyer dafür gehalten, sich endlich offen zu einer Privatrechtswirkung der Grundrechte zu bekennen, vgl. *ders.*, Horizontalwirkung im Vergleich: Ein Plädoyer für die Geltung der Grundrechte zwischen Privaten, Tübingen 2020.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Trennung zwischen öffentlichem und privatem Recht, die im 19. Jahrhundert mit großem Aufwand herausgearbeitet[25] wurde? Diese Fragen werden uns in den kommenden Jahren sicherlich beschäftigen. Dass sie sich im Moment in dieser Form stellen, macht jedenfalls schon einmal auf eines aufmerksam: dass diese Trennung weniger selbstverständlich als vielmehr äußerst voraussetzungsreich war. Und das bedeutet nicht, dass sie nicht stets, gerade auch unter Einfluss des Common Law und des Unionsrechts, wieder in Frage gestellt werden kann.[26]

b) Rechtsakte der Europäischen Union

Jenseits solcher (fundamentale und ganz große Linien verfolgenden) Debatten war es bislang die Gerichtsbarkeit, die die wesentlichen Pfeiler in den „digitalen Raum" eingezogen hat.[27] Es bleibt aber zu fragen, ob die dritte Gewalt wirklich dauerhaft der Ort sein soll, an dem die mit der digitalen Souveränität aufgeworfenen Fragen reflektiert werden. Aus Gründen der Gewaltenteilung und der demokratischen Legitimation kann die Antwort eigentlich nur „nein" lauten. Aufgerufen ist vielmehr der Gesetzgeber. Der Souverän ist, auch im Internetzeitalter, in der parlamentarischen Demokratie immer noch das Staatsvolk, und das Parlament ist zu seiner Vertretung *unmittelbar* legitimiert.[28] Und in der Tat hat der Deutsche Bundestag in Form des Netzwerkdurchsetzungsgesetzes und seiner Überarbei-

25 Die Diskussion findet sich intensiv nachgezeichnet bei *Stolleis*, Geschichte des öffentlichen Rechts in Deutschland, Bd. 2, München 1992; vgl. dazu auch *Grimm*, Zur politischen Funktion der Trennung von öffentlichem und privatem Recht in Deutschland, in: ders., Recht und Staat der bürgerlichen Gesellschaft, Frankfurt a.M. 1972, S. 84-161.

26 Dazu *Grimm*, Das Öffentliche Recht vor der Frage nach seiner Identität, Tübingen 2012, S. 1 ff.; *Seckelmann*, Kategoriale Unterscheidung zwischen Öffentlichem Recht und Privatrecht?, Begleitaufsatz zur 79. Jahrestagung der Vereinigung der Deutschen Staatsrechtslehrer, DVBl 2019, 1107-1116.

27 Diese Formulierung aus der Antrittsvorlesung von 2022 wurde auf dem Originalstand belassen; inzwischen sind die auf den nächsten beiden Seiten dargestellten unionalen Rechtsakte ergangen.

28 Vgl. nur *Sommermann*, in: Huber/Voßkuhle (Hrsg.) (vormals von Mangoldt/Klein/Starck), Grundgesetz – Kommentar, 8. Aufl., München 2024, Art. 20 Rn. 156; bezogen auf ein mögliches Legitimationsmodell für die EU vgl. *von Achenbach*, Demokratische Gesetzgebung in der Europäischen Union: Theorie und Praxis der dualen Legitimationsstruktur europäischer Hoheitsgewalt, Berlin/Heidelberg 2014.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

tung versucht, rechtliche Standards „freier" Kommunikation im Internet zu etablieren.[29]

Allerdings – und auch das wäre für die Rechtswissenschaft des 19. Jahrhunderts kaum vorstellbar gewesen – ist der nationale Gesetzgeber kaum noch in der Lage, ein solches Mammutvorhaben zu stemmen. Die Einhegung der systemischen Risiken, die von den Gatekeepern ausgehen, unternimmt jetzt vielmehr die Europäische Union im Rahmen ihrer „Digitalen Agenda", die auch dem Aufbau einer „Digitalverfassung" dienen soll.[30] Diese wird – so ist jetzt schon zu prognostizieren – Inhalt meiner Lehre in Hannover in den nächsten Jahren sein.

Wenn die Europäische Union im digitalen Raum von verschiedenen Seiten in ihrer Souveränität bedroht wird, so liegt es nahe, ihr auch eine „digitale" Verfassung zu geben. Damit könnte auch die Frage von Gunther Teubner und Angelo Golia beantwortet werden, „ob und wie grundlegende verfassungsrechtliche Prinzipien – insbesondere Gewaltenteilung, Demokratie, Grundrechte und Rechtsstaatlichkeit – auch in der digitalen Welt Geltung erlangen können".[31] Es handelt sich bei der „Digitalverfassung" allerdings um kein geschlossenes Verfassungsdokument. Vielmehr ist damit ein mosaikartiges System aus verschiedenen Verordnungen („Acts" genannt) gemeint, die das europäische Datenrecht betreffen.

In diesem Zusammenhang seien nur die Europäische „Verordnung über einen Binnenmarkt für digitale Dienste" (kurz: „Gesetz über digitale Dienste"[32] bzw. „Digital Services Act", DSA) und die „Verordnung über bestreitbare und faire Märkte im digitalen Sektor" (oder kurz: „Gesetz über digitale Märkte"[33] bzw. „Digital Markets Act", DMA) genannt. Namentlich die letztgenannte Verordnung reflektiert die Möglichkeit der Anballung enormer

29 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz) vom 1. September 2017 (BGBl. I S. 3352), zuletzt geändert durch Artikel 3 des Gesetzes vom 21. Juli 2022 (BGBl. I S. 1182).

30 Einen Baustein zu einer digitalen Grundrechtecharta bilden die „digitalen Grundsätze", vgl. *Europäische Kommission*, Mitteilung: Eine europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade, 26.1.2022, COM/2022/27 final; zur „digitalen Dekade" allgemein vgl. *Mehde*, Der unionale Rahmen von E-Government, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung (Fn. 15), S. 301-321.

31 *Teubner/Golia*, Digitalverfassung, JZ 2023, 625-630 (625).

32 VO (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, ABl. L 277 vom 27.10.2022.

33 VO (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Macht bei den Gatekeepern. So spricht Erwägungsgrund 3 zum DMA davon, dass „[e]inige wenige große Unternehmen, die zentrale Plattformdienste bereitstellen, [...] beträchtliche wirtschaftliche Macht erlangt" hätten. Allerdings ist der Digital Markets Act auf die Freihaltung des europäischen Binnenmarkts gerichtet und verfolgt damit eher einen kartellrechtlichen Ansatz. Die Frage einer Verpflichtung der Gatekeeper wird daher eher durch den Digital Services Act adressiert. In seinem Erwägungsgrund 35 findet sich dann auch eine direkte Bezugnahme auf die Grundrechte-Charta.[34] Zusammen mit dem sog. Data Governance Act,[35] dem Data Act[36] und dem AI Act[37] bilden diese Normen ein Paket, mit welchem der EU-Gesetzgeber seiner Schutzpflicht aus den Verbürgungen der Art. 7 und 8 der Grundrechtecharta der Europäischen Union (Achtung des Privat- und Familienlebens bzw. Schutz personenbezogener Daten) nachkommt.

### c) GAIA X und sichere Identitätsökosysteme

Der Digitalstrategie der Europäischen Union zufolge sollen überdies nicht nur die Zugangswege offengehalten werden. Vielmehr soll parallel eine leistungsfähige, sichere und damit vertrauenswürdige europäische Dateninfrastruktur aufgebaut werden – genau diese ist, wie gesagt, Gegenstand des GAIA X-Programms.

Es geht also um nichts weniger als um ein europäisches Datenökosystem. So schön sie klingt: Diese „ökologische" Metapher ist nicht ganz unproblematisch. Denn sie verschleiert die Frage danach, wer letztlich darüber ent-

---

der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. 265/1 vom 12.10.2022.

34 Genauer gesagt handelt es sich wohl um die gesetzgeberische Konkretisierung einer Schutzpflicht, dazu bereits *Gusy*, Grundrechtsbindungen Privater (Fn. 23).

35 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. L 152/1.

36 VO (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung), ABl. L 2023/2854 vom 22.12.2023.

37 VO (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, ABl. L 2024/1689 vom 12.7.2024.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

scheidet, wie sich Bürgerinnen und Bürger „selbstsouverän" der Verwaltung gegenüber legitimieren können.[38]

Hierbei handelt es sich jedoch um den *springenden Punkt des digitalisierten Verwaltungsrechts*. Deutlich wird die Notwendigkeit eines digitalen Berechtigungsmanagements zum Beispiel bei der Beantragung einer Baugenehmigung. Denn, im Unterschied zum „Brötchenkauf", also einem Alltagsgeschäft mit Barzahlung, ist bei der Stellung eines Bauantrags die Identität des Antragstellenden dem Gegenüber nicht egal. So verlangt § 53 Abs. 3 der Niedersächsischen Bauordnung eine Bauvorlageberechtigung. Die nachzuweisende Bauvorlageberechtigung als Entwurfsverfasser können laut den Absätzen 3 bis 5 von § 53 NBauO je nach Vorhaben nur Architekten, Innenarchitekten oder Prüfingenieure innehaben.

Wie können Sie sich dabei legitimieren, wenn die Behörde nicht erkennen kann, wer ihr „digital gegenübersitzt"? Der sichere Identitätsnachweis nach § 18 des Personalausweisgesetzes kann etwa dadurch geführt werden, dass man die Chipkarte an seinem Personalausweis aktiviert hat und diesen in ein Lesegerät einführt. Architektinnen bzw. Architekten verfügen zumeist über solche Kartenlesegeräte. Jedoch werden die wenigsten von uns bei sich zuhause ein solches Lesegerät haben. Daher wäre es schön, wenn man den Personalausweis einfach in einer elektronischen Brieftasche, einer sogenannten Wallet, in seinem Smartphone hinterlegen könnte. Dort könnte man dann auch andere Berechtigungsnachweise speichern, etwa einen Angelschein. Erste Versuche dazu werden bereits pilothaft in Deutschland durchgeführt.[39] Auch die Europäische Union plant im Rahmen der Novellierung der eIDAS-Verordnung[40] die Einrichtung einer „Europäischen Digitalen Identität", die im Rahmen einer „europäischen" Wallet abgelegt werden kann.[41]

38 Dazu (etwas polemisch) *Aretz*, Der Souverän in der Krise: Gedanken zur Reichweite der Macht über die eigenen Identitätsdaten, DuD 2022, 40-44.

39 Dazu *Brunzel/Reutner/Seckelmann*, Sichere digitale Identitäten als Fundament datenzentrierter Verwaltungsinformatik, VM 2023, 280-285.

40 VO (EU) 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257/73 vom 28.8.2014.

41 Dazu Näheres unter https://digital-strategy.ec.europa.eu/en/policies/electronic-identification bzw. https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox (beides zuletzt abgerufen am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Und hier kommen wir zu einem der Souveränitätsbegriffe, die ich eingangs zunächst ausgeklammert hatte, nämlich dem *selbstsouveränen* Umgang der Nutzerinnen und Nutzer mit den elektronisch in ihrer Wallet gespeicherten Dokumenten. Diesen datenschutzkonformen Umgang sicherzustellen, ist allerdings voraussetzungsreich: Damit das umgesetzt werden kann, muss auf dem Smartphone ein geschützter Bereich existieren, auf den niemand anderes, auch und gerade nicht irgendein Geheimdienst, zugreifen kann.[42] Allerdings sind nahezu alle Akteure entweder in kalifornischer oder in chinesischer Hand: Während Google und Huawei Android benutzen, hat Apple ein eigenes Betriebssystem. Alle lassen aber, das haben die beiden Schrems-Entscheidungen des EuGH[43] deutlich vor Augen geführt, eine sogenannte Backdoor für Geheimdienste. Google und Apple tun das für die amerikanischen Sicherheitsdienste– und davon, dass Huawei das in Bezug auf China tut, ist auszugehen.

Eines der entscheidenden Probleme des deutschen E-Governments lässt sich an diesem Beispiel festmachen: Will der Staat ein selbstsouveränes Identitätsmanagement der Bürgerinnen und Bürger zulassen, so muss es ihm gelingen, in einem *nicht-souveränen Identitätssystem eine selbstsouveräne Wallet* einzurichten. Das allerdings gleicht einer Quadratur des Kreises.

Genau darum bemüht sich aber das bereits erwähnte europäische GAIAX-Programm. Es will sichere (in bestimmten Themenfeldern verbundene) Identitätenökoysteme aufbauen und setzt dabei auf ein sogenanntes *Secure Element*: In die elektronischen Geräte – beispielsweise das Smartphone – soll eine SIM-Karte eingebaut werden, die dafür sorgt, dass die elektronischen Dokumente verschlüsselt werden und nur durch den Berechtigten bzw. denjenigen, denen er seinen privaten Schlüssel offenbarte, gelesen werden können. Der Samsung-Konzern, auf dessen Geräten auch Android läuft, hat sich hierfür offen gezeigt und zugelassen, dass auf seinen Smartphones ein entsprechendes Secure Element installiert wird.[44] Dieses wurde im Rahmen des Optimos-Projekts von einem Projektkonsortium unter Federführung der Bundesdruckerei entwickelt. Zwar ist hierfür ein relativ neues Samsung-Smartphone erforderlich – aber immerhin.

---

42 Zur Funktionsweise vgl. *Puhl/Roloff/Märkel/Lundborg*, Digitale Identitäten als Fundament des Web 3.0, WIK Diskussionsbeitrag, No. 503, Bad Honnef 2023.

43 EuGH Urt. v. 6.10.2015 – C-362/14 – Schrems I bzw. EuGH Urt. v. 16.7.2020 – C 311/18 – Schrems II.

44 https://news.samsung.com/de/sicher-und-einfach-identifizieren-mit-dem-smartphone (zuletzt abgerufen am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

Ein ganz ähnlicher Kampf um Selbstbehauptung und Deutungshoheit findet zurzeit in Bezug auf die Cloud-Strukturen statt. Hier ist vor allem die *deutsche Verwaltungscloud* zu nennen, die von Bund und Ländern etabliert werden soll.[45]

Mit ihr sollen vor allem die Cloud-Lösungen von Bund, Länder und Kommunen miteinander kompatibel gemacht werden. Auch das ist ein zentraler Punkt. Eben weil die Clouds bislang nicht durchgängig kompatibel sind, weichen Bund und Länder momentan noch oft auf kommerzielle Angebote wie die Azure-Plattform von Microsoft aus. Diese haben aber nicht nur die genannten datenschutzrechtlichen Nachteile. Es droht ein Vendor-Lock-In-Effekt: Hat man seine Daten in einer bestimmten Cloud abgelegt, wird ein Umzug zu einer anderen Cloud-Lösung immer schwieriger. Und kritische Abhängigkeiten der deutschen Verwaltung von den kalifornischen Hyperscalern drohen erneut.

### d) Interoperabilitätsstandards

Die Lösung besteht nunmehr darin, *Schnittstellen* zu definieren, um die föderalen Cloud-Lösungen miteinander interoperabel und kompatibel zu machen. Entscheidend ist nun, wer die Interoperabilitätsstandards definiert. Diese Funktion nimmt in der Bundesrepublik Deutschland der IT-Planungsrat wahr, der aufgrund eines Staatsvertrags nach Art. 91c Abs. 1 und 2 GG als Bund-Länder-Gremium eingerichtet wurde. In ihm sind die *Chief Digital Officers* von Bund und Ländern vertreten.[46] Und er soll es sein, der im Rahmen der deutschen Verwaltungscloudstrategie die Architekturvorgaben zur Entwicklung von Anwendungen erlässt, die für private wie öffentliche Dienstleister gelten sollen, wenn sie Services für die deutsche Verwaltung entwickeln.

Um zum Ausgangspunkt zurückzukommen: Ist die Definitionsmacht über Interoperabilitätsstandards ein Element staatlicher Souveränität? Oder andersherum gefragt: Kann man staatliche Souveränität im Internetzeitalter denken, ohne dass die Macht zur Standarddefinition für E-Govern-

45 https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html (zuletzt abgerufen am 29.2.2024).

46 Zur Zusammensetzung und den Aufgaben des IT-Planungsrats vgl. *Lühr*, Der IT-Planungsrat, Bremen 2023.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

ment-Anwendungen beim Staat liegt? Wohl eher nein. Nimmt man die klassische Definition staatlicher Souveränität von *Jean Bodin*, so ist es die unbeschränkte, unvermittelte Möglichkeit zur Herrschaftsausübung über die Untertanen. Und nach der moderneren Drei-Elemente-Lehre *Georg Jellineks* bedarf ein Staat eines Staatsvolks, eines Staatsgebiets und einer Staatsgewalt.[47] Letztere meint die Möglichkeit zur Ausübung hoheitlicher Macht ohne Einschaltung vermittelnder Instanzen.

Und diese gibt es im *Electronic Government* auf einer fortgeschrittenen Stufe eben nur dann, wenn es eine anbieterunabhängige sichere Aufbewahrungsmöglichkeit verwaltungsrelevanter Dokumente in einer selbstsouveränen Wallet gibt. Diese bildet die Basis der Kommunikation zwischen den Bürgerinnen bzw. Bürgern und der Verwaltung, ohne dass jemand anderes ungefragt Einsicht nehmen kann. Und an dieser Stelle berühren sich die Selbstsouveränität der Nutzenden und die staatliche Souveränität. Letztere wäre dann bedroht, wenn es Mittelsmänner geben würde, sogenannte Intermediäre oder Türhüter, die nach gänzlich eigenem Ermessen[48] darüber entscheiden könnten, wem sie wann den Zugang zu zentralen Kommunikationskanälen gewähren.

Ob es nach allem nicht günstiger ist, sich bei häufigen Verwaltungskontakten ein Lesegerät für den digitalen Personalausweis zuzulegen, wäre ebenfalls eine berechtigte Frage. Die IT-Sicherheitsexpertin *Lilith Wittmann* hat vor einiger Zeit genau das thematisiert,[49] frei nach dem Motto „Warum kompliziert, wenn es auch einfach geht?"

Und tatsächlich gilt: Wenn mehr Bürgerinnen und Bürger von der eID-Funktion ihres Personalausweises Gebrauch machen würden, könnte man sich die schwierige Suche nach weiteren fälschungssicheren Identitätsnachweisen sparen.

## 4. Entstehen einer neuen Staatsaufgabe?

Nochmals zurück zum Vortragstitel: Ist die Möglichkeit zur Definition von Interoperabilitätsstandards ein – neues oder vielleicht sogar implizit

47 *Jellinek*, Allgemeine Staatslehre, 3. Aufl., Berlin 1914, S. 394.

48 Hier setzen der Digital Services Act und der Digital Markets Act an.

49 *Wittmann*, Mit der ID-Wallet kannst Du alles und jeder sein, außer Du musst Dich ausweisen, Posting v. 29.9.2021 unter https://lilithwittmann.medium.com/mit-der-id-wallet-kannst-du-alles-und-jeder-sein-außer-du-musst-dich-ausweisen-829293739fa0 (zuletzt abgerufen am 29.2.2024).



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

mitgeregeltes – Element staatlicher Souveränität? Die Antwort muss wohl lauten: ja.

Wenn man will, kann frei nach *Christian Ernst* in der Gewährleistung digitaler Souveränität eine neue, ungeschriebene Staatsaufgabe sehen.[50] Man könnte sozusagen einen Kern definieren, in dem die Aufgabe vom Staat sowohl verantwortet als auch bewirkt werden muss. Hierzu möchte ich die *Definition der Interoperabilitätsstandards* rechnen. Um diesen engen Kern herum ließe sich ein *weites Feld* abstecken, das man als Gewährleistung sicherer und vertraulicher Bürger-Staat-Kommunikation definieren kann. Zu dessen Herleitung ließe sich die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 zum sogenannten Computer-Grundrecht anführen.[51] Diese war zwar abwehrrechtlich gemeint, könnte sich aber ggf. auch dahingehend interpretieren lassen, dass Schutzdimensionen aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG aktiviert werden.

Wie nun soll diese Verpflichtung wahrgenommen werden? Man könnte für dieses weitere Feld einmal wieder den Gedanken einer Gewährleistungsverantwortung konstruieren, in diese Richtung lässt sich auch der Vorschlag von *Christian Ernst* zum Grundsatz digitaler Souveränität verstehen.[52] Wir kennen den Gedanken aus der Privatisierungsdiskussion der 1990er und 2000er Jahre. Bezogen auf die heutigen und hier behandelten Fragen lässt er sich folgendermaßen begreifen: Der Staat hat – jenseits der Definition von Sicherheits- und Interoperabilitätsstandards – nicht alles selbst zu erfüllen, wohl aber eine grundrechtskonforme Erfüllung zu gewährleisten. Das kann durch öffentlich-rechtliche Einrichtungen wie Dataport als Anstalt des öffentlichen Rechts erfolgen oder im Wege einer Beleihung geschehen beziehungsweise durch Öffentlich-Private Partnerschaften.

Man kann im Zeichen digitaler Souveränität also erneut in Verantwortungsstufen[53] denken: Es gibt einen harten Kern, bei dem die entsprechen-

50 *Ernst*, Der Grundsatz digitaler Souveränität: Eine Untersuchung zur Zulässigkeit des Einbindens privater IT-Dienstleister in die Aufgabenwahrnehmung der öffentlichen Verwaltung, Berlin 2020.

51 Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme, BVerfG vom 27.2.2008, BVerfGE 120, 274.

52 *Ernst*, Digitale Souveränität (Fn. 50).

53 *Schuppert*, Die öffentliche Gewalt im Kooperationsspektrum staatlicher und privater Aufgabenerfüllung: Zum Denken in Verantwortungsstufen, VERW 1998, 415-447; vgl. auch *Knauff*, Der Gewährleistungsstaat: Reform der Daseinsvorsorge – Eine rechtswissenschaftliche Untersuchung unter besonderer Berücksichtigung des ÖPNV, Berlin 2004.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

de Staatsaufgabe auch vom Staat erfüllt werden muss. Dieser Kern hat ein Umfeld, in dem Gewährleistung und Erfüllung auseinanderfallen können.

Versteht man den Begriff der „digitalen Souveränität" in dieser Weise, markiert er nicht lediglich einen Kampfbegriff, mit dessen Hilfe private Anbieter vom Markt verdrängt werden sollen, wie es die kalifornischen Hyperscaler der Europäischen Union und ihren Mitgliedstaaten unterstellen. Vielmehr kann er als Leitlinie zur Markierung der verschiedenen Verantwortungsstufen und damit auch als eine Art roter Faden bei der Neuvermessung von Staatlichkeit im „digitalen Raum" dienen.

## III. Fazit und Ausblick

Abschließend ist Folgendes festzuhalten: Der Begriff der digitalen Souveränität steht für einen Funktionswandel des Staates im Internetzeitalter, den man – in Analogie zur IT-Diktion – als Wahrnehmung der Rolle eines *Trusted Service Managers* beschreiben kann,[54] welcher die entscheidenden Schnittstellen definiert und zugleich ihre Bereitstellung gewährleistet.

Durch die Differenzierung der verschiedenen Rollen oder Funktionen der *Definition* von Standards und der *Bereitstellung* von Möglichkeiten wird das Modell des Gewährleistungsstaates neu aktiviert und mit Leben gefüllt.

Während der Staat (also Bund und Länder, repräsentiert in Bund-Länder-Gremien wie dem IT-Planungsrat) die *Definition* von Standards *selbst* vorzunehmen hat, kann er hinsichtlich der Sicherstellung der Vertraulichkeit und Integrität wie ein neutraler Broker agieren, dem zugleich das „Interdependenzmanagement"[55] obliegt.

Und schließlich: Wenn der Staat die Erfüllung desselben an Private oder an Öffentlich-Private Partnerschaften überträgt, so hat er diese nicht nur auf die von ihm (etwa im Wege eines Pflichtenheftes) definierten Standards zu verpflichten, sondern auch Rückholoptionen vorzusehen.[56] Denn so können die Lehren integriert werden, die aus der Privatisierungsdiskussion der 1990er und 2000er Jahre zu ziehen sind. Das bedeutet konkret, dass

54 Eine ähnliche Analogie zu einer früheren Diktion hat *Augsberg* (Der Staat als Informationsmittler – Robin Hood oder Parasit der Wissensgesellschaft?, DVBl 2007, 733-741) gebildet.

55 Begriff nach *Mayntz*, Gesellschaftliche Modernisierung und die veränderte Rolle des Staates, in: Max-Planck-Gesellschaft (Hrsg.), Jahrbuch 1995, Göttingen 1996, S. 57-70.

56 Dazu *Wollenschläger*, Effektive staatliche Rückholoptionen bei gesellschaftlicher Schlechterfüllung, Baden-Baden 2006; *Seckelmann*, Evaluation und Recht, Tübingen 2018, S. 47, 216 und 410.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY

bei der Verwaltung genug Know-how vorhanden sein muss, um das Pflichtenheft, die Aufsicht und ggf. die Rückholung selbst bewerkstelligen zu können. So banal das klingt, so wenig selbstverständlich ist es. Und das hängt mit der personellen „Ausblutung" der Kommunalverwaltung zusammen, die zudem die Last der Umsetzung des Onlinezugangsgesetzes zu stemmen hat.

Eine kurze Gesamtbilanz zur digitalen Transformation kann daher lauten: Wir müssen Staatlichkeit im „digitalen Raum" neu denken. Der Begriff der „digitalen Souveränität", wie ihn die Europäische Union und der deutsche Staat geprägt haben, ist schillernd, da sein Bezugspunkt nicht ganz klar ist: Richtet er sich gegen andere Staaten oder aber gegen Wirtschaftsunternehmen, von denen man abhängig zu werden droht – oder wendet er sich möglicherweise nur gegen nichteuropäische Wirtschaftsunternehmen, von denen man abhängig zu werden droht? Eines jedenfalls ist klar: Die Träume der 1990er Jahre von einem freien Internet, in dem das selbstgeschaffene Recht der Wirtschaft autonom zur Geltung kommt, sind ausgeträumt. Die „*lex mercatoria*" Gunther Teubners[57] ist der Zusammenballung wirtschaftlicher Macht und den staatlichen Reaktionen darauf zum Opfer gefallen.[58]

57 *Teubner*, Globale Bukowina: Zur Emergenz eines transnationalen Rechtspluralismus, Rechtshistorisches Journal 15 (1996), 255-290.

58 Eine solche Entwicklung ließe sich, bezogen auf neue Inventionen, für das ausgehende 19. und frühe 20. Jahrhundert nachzeichnen, dazu *Seckelmann*, Industrialisierung, Internationalisierung und Patentrecht im Deutschen Reich, 1871-1914, Frankfurt a.M. 2006, S. 195 ff.



https://doi.org/10.5771/9783748949893-391 https://www.inlibra.com/de/page/agb - Open Access - (cc) BY