Europas Digitale Souveränität als Ziel und Prüfstein des Datenprivatrechts

Michael Denga

Entwurf

A. Datenkommerz und Souveränität

Europa sucht nach ihrer Digitalen Souveränität. Längst werden essentielle Dienstleistungen der Wissensgesellschaft nicht mehr von Europäischen Unternehmen oder von Europäischem Boden aus erbracht. Fast zwingend geht damit einher, dass die Deutungshoheit über die neu entstandenen digitalen Räume in vielerlei Hinsicht nicht bei der EU, ihren Mitgliedstaaten, ihren Unternehmen oder Bürgern liegt. Dies wird als faktische Fremdbestimmung wahrgenommen – und als gesellschaftliches Risiko. Auf den Kontrollverlust reagiert die EU mit umfassender Regulierung, die freilich nicht immer den eigenen Idealen gerecht wird. Insbesondere wird die Selbstbestimmung der Unternehmen und Bürger – die Privatautonomie, oder auch: digitale Selbstbestimmung – nur unzureichend gewahrt und gewürdigt. Anhand eines zentralen Rechtsproblems der digitalen Wirtschaft und Gesellschaft soll diese These genauer überprüft werden: der Kommerzialisierung personenbezogener Daten.

Das digitale Geschäftsmodell „Dienst gegen Daten“ hat sich fraglos durchgesetzt. Hier hat der Europäische Gesetzgeber mit der Datenschutzgrundverordnung und den beiden neueren Richtlinien über den Warenkauf und digitale Inhalte versucht, die Position der Kunden zu verbessern. Die Kunden digitaler Anbieter wurden mit umfangreichen „Datenrechten“ ausgestattet; vor allem ist das Konzept von „Daten als Gegenleistung“ dadurch nun endgültig rechtlich anerkannt.

Allerdings stehen noch viele Probleme im Raum, die einen wirklich privatautonomen Gebrauch der Datenrechte und damit auch ein echtes Kräftegleichgewicht zwischen europäischen Kunden und internationalen Unternehmen verhindern. An dieser Stelle ist die Rolle Digitaler Souveränität relevant, die ein prominenter Diskursbegriff ist und sich zugleich durchaus negativ auf die selbstbestimmte Datenhoheit auszuwirken scheint.

B. Datenkontrolle unter der DSGVO

Die DSGVO ist Hauptinstrument der EU für die Umsetzung ihres Anspruchs auf Digitale Souveränität; gleichzeitig beruht die DSGVO auf dem Gedanken dezentraler Ordnung durch privatautonome Akteure.

I. Verschärfung der Wirksamkeit des Datenschutzes durch die DSGVO

Die EU hat 2018 durch die DSGVO die für die EU maßgeblichen Datenschutzstandards erheblich verschärft. Zwar mögen die materiell-rechtlichen Grundkonzepte im Wesentlichen unverändert geblieben sein, da schon die Datenschutz-Richtlinie 95/46/EG das Verbot der Verarbeitung personenbezogener Daten unter Erlaubnisvorbehalt stellte. Allerdings wurden im Detail weitaus höhere Anforderungen an die Erlaubnistatbestände festgelegt, sowie insbesondere das Durchsetzungsdefizit unter der Datenschutz-Richtlinie durch verschärfte Sanktionen und erweiterten Schuldnerkreis adressiert. Zudem wurde das sog. *Marktortprinzip* für die internationale Geltung der DSGVO eingeführt, wonach diese jeden erfasst, der Leistungen im Binnenmarkt der EU anbietet und dabei personenbezogene Daten von in der EU befindlichen Personen verarbeitet. Man kann also durchaus davon sprechen, dass mit der DSGVO ein Ausrufezeichen für den Kontrollwillen der EU über die Datenwirtschaft gesetzt wurde.

II. Dezentrale Datenallokation als Fundament der Europäischen Datenordnung

Die DSGVO wird hybrid durchgesetzt, zum einen durch behördliche Aufsicht und Sanktion, zum anderen durch private Gestaltungsrechte und Schadensersatzansprüche. Kern der Datenordnung ist jedoch klar die private, dezentrale Allokation durch Zuordnung der Verfügungsbefugnis über personenbezogene Daten an die einzelnen Marktteilnehmer.

Das Primat autonomer Entscheidung ist Fundament des Europäischen Privatrechts und muss auch bei komplexen Technologieanwendungen zum Tragen kommen, denn die freie Entscheidung im Vertragsschluss ist Grundlage der europäischen Marktwirtschaft, sie liegt dem Gedanken effizienter Ressourcenallokation im dezentralen Marktgeschehen zu Grunde, ein Gedanke der insbesondere von der ordoliberalen Schule und deren Vertreter *August von Hayek* geprägt wurde. Letztendlich ist der gesamte Binnenmarkt der EU als dezentrale, das heißt staatsfreie Austauschordnung konzipiert, welche es dem Einzelnen erlauben soll, ohne staatliche (und teilweise auch private) Barrieren am Markt zu partizipieren.

Dieses solide Grundkonzept der dezentralen Datendistribution durch die privaten Marktakteure leidet jedoch sowohl an der konkreten Umsetzung als auch an der Missachtung der Funktionsbedingungen privatautonomer Entscheidungen.

C. Probleme der Datenkommerzialisierung

Die Ermöglichungsfunktion im europäischen Datenprivatrecht in Hinblick auf Datenkommerzialisierung ist bislang eher schwach ausgeprägt.

I. Rechtliche Unsicherheiten bei Datenverfügungen

Die Datenwirtschaft leidet erheblich unter rechtlichen Unsicherheiten bei Verfügungen über personenbezogene Daten, die in einer sehr großen Vielzahl von Fällen betroffen sein können, so dass der Anwendungsbereich der DSGVO teils unvorhersehbar und jedenfalls häufig eröffnet ist.

Wirksamkeitsvoraussetzung ist unter beiden privatautonomen Legitimierungsgrundlagen, dass die beabsichtigten Zwecke der Datenerhebung hinreichend bestimmt bezeichnet sind und die Weiterverarbeitung in einer mit diesen Zwecken zu vereinbarenden Weise erfolgt, Art. 5 Abs. 1 b) DS-GVO. Zentral ist auch der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 c) DSGVO, wonach die Zwecke der Datenverarbeitung angemessen und erheblich sein müssen, sowie die Verarbeitung auf das für diese Zwecke erforderliche Maß beschränkt.

Beide Prinzipien stehen insbesondere Blankoermächtigungen und pauschalen Erklärungen entgegen. Das bedeutet für den Sekundärmarkt – den Datenhandel nach der primären Datenerhebung –, dass insbesondere der Personenkreis, an den die Daten weitergegeben werden sollen, und dessen Verarbeitungszwecke hinreichend klar eingegrenzt sein müssen. Ein freier, spontaner Handel personenbezogener Daten mit anonymen Käufern zu deren autonomen Verarbeitungszielen ist daher nicht möglich.

II. Paternalismus statt Nutzerpräferenzen?

Wie schwer die rechtlichen Hürden für die Verarbeitung und Weitervermarktung von personenbezogenen Daten tatsächlich wiegen, ist freilich kaum zu erfassen – jedenfalls haben sich die **Börsenwerte großer Plattformunternehmen** seit Einführung der DSGVO nicht verschlechtert, sondern im Fall von *Meta* und *Alphabet* bis zum zweiten Quartal 2022 gar verdoppelt, und es kam sogar zum erfolgreichen Börsengang eines Datenhändlers, *Palantir*.

Der unbestrittene Erfolg von Plattformunternehmen der Aufmerksamkeitsökonomie belegt vor allem die einem strengen Schutz personenbezogener Daten entgegenlaufenden Nutzergewohnheiten. Die Nachfrage nach Kostenlosprodukten im Internet ist ungebremst und Bezahlmodelle konnten sich bislang nicht durchsetzen. Eine massenhafte Durchsetzung der Nutzerrechte und Wirksamkeitsbedingungen unter der DSGVO ist bislang jedenfalls durch die Nutzer nicht erfolgt.

Die Divergenz zwischen Schutzzielen und Praxis des Datenrechts wird verhaltensökonomisch als ***Privacy Paradox*** erfasst und hat den Europäischen Gesetzgeber dazu bewogen, die Datenverwertung und Teilhabe an den wirtschaftlichen Chancen der Datenökonomie stärker in den Blick zu nehmen.

III. Informationsdefizite

Allein eine formale Wahlfreiheit über Datentransaktionen reicht nicht hin, vielmehr müssen ihre Grundlagen geschaffen werden; dabei ist davon auszugehen, dass auch bereits eine minimale Informationsgrundlage hinreicht, um eine authentische autonome Entscheidung zu ermöglichen.

In der Tat offenbaren sich wirtschaftliche und informationelle Asymmetrien zwischen Datensubjekten und größeren Unternehmen der Datenwirtschaft. Zentral ist dabei, dass der Wert personenbezogener Daten häufig nicht gleichermaßen klar ist, wie der Wert monetärer Rechnungseinheiten.

Paradigmatisch lässt sich dies am Beispiel der Cookie-Zustimmungsabfragen veranschaulichen, welche längst die Lästigkeitsschwelle überschritten haben und daher weder eine Warnfunktion erfüllen noch eine rationale Abwägungsentscheidung befördern. Die massenhafte Erhöhung von Verhandlungskosten für nicht immer wesentliche Interaktionen führt zu einer Abnutzung der Informationsfunktion der Zustimmungsabfragen. Zu dieser Überforderungssituation tritt der Einsatz manipulativer *Dark Pattern*, welche zunehmend durch kognitive Verzerrungen die Nutzerentscheidungen beeinflussen.

Die Zumutung dieser Schwierigkeiten deutet darauf hin, dass das Nutzerwohl und seine privatautonome Verwirklichung nicht alleine im Zentrum des europäischen Datenprivatrechts stehen.

IV. Reduktion der Gesamtwohlfahrt

Das zentrale Problem der Datenökonomie ist, dass Daten bislang zu wenig geteilt werden. „Big Data“ wird die Fähigkeit zugeschrieben, die großen gesellschaftlichen Probleme, vom Strapenverkehr über die Finanzmarktstabilität bis hin zum Klimawandel, durch überlegene statistische Analyseleistung zu lösen. Prämisse der visionären Anwendungsprognosen – und auch von weniger ambitionierten Geschäftsmodellen – ist allerdings die unumschränkte Nutzbarkeit und die reibungslose Allokation aller jemals generierten Daten an die für die jeweilige Datenart und –qualität optimale Verarbeitungsstelle. Hierzu steht jede Art von Transaktionshindernis quer, zumal das die DSGVO beherrschende Grundkonzept von Verbot mit Erlaubnisvorbehalt. Die

grundsätzliche Frage des Datenzugangs ist essentiell für die algorithmische Förderung von Gemeinwohlbelangen; hier scheint ein „Datenegoismus“ nun im Bereich personenbezogener Daten auch durch eine formelle Position gefördert, was insbesondere marktmächtigen Unternehmen zu Gute kommt und Wettbewerb verhindert. Dies wiederspricht im Grundsatz der staatlichen Infrastrukturverantwortung, welche auf Wettbewerb und Verbraucherschutz gleichermaßen ausgerichtet ist.

Der ethische Imperativ der Beschränkung allgemeiner Datenfluktuation ist zwar indiskutabel; dennoch scheint es misslich, wenn die Datenschutzordnung die möglichen Gemeinwohlsteigerungen in einem Maße behindert, wie es sich nicht aus dem zum Schutze personenbezogener Daten Erforderlichen ergibt. Die oben beschriebenen Erschwernisse und Unsicherheiten bei Datentransaktionen, allerdings auch gerade die Schwierigkeiten für den einzelnen Rechtsträger bei der Ausübung seiner Rechte in Angesicht ausufernder, intransparenter Datenschutzerklärungen – viel diskutiert unter dem Stichwort „Information Overload“ – verhindern gerade eine Transaktionseffizienz im Rahmen der prinzipiellen Beschränkungen privaten Datenverkehrs. Vielmehr ist ein erhebliches Lästigkeitspotential durch die bis ins dritte und vierte Glied reichenden Compliance-Anforderungen festzustellen, welche zwar nicht Datentransaktionen völlig unterbindet, sie indes doch erheblicher langsam macht und jede gutwillige Nutzersorgfalt durch ständige Abfrage dezimiert, zu beobachten ist eine Praxis des „click and forget“.

D. Kaum spürbare Besserungen im neueren Datenwirtschaftsrecht

Auch die neueren Rechtsakte der EU zur Datenwirtschaft (im zweiten Quartal 2022 noch im Entwurfsstadium), welche dezidiert dem Ziel dienen, den Binnenmarkt für Daten zu fördern, der Data Governance Act sowie der Data Act, tragen kaum zur Entlastung in der Datenwirtschaft bei.

I. Datenintermediation unter dem Data Governance Act

Mit dem vom EU-Parlament im April 2022 beschlossenen Data-Governance-Act (DGA) soll die privatautonome Weitergabe insbesondere von personenbezogenen Daten und Geschäftsgeheimnissen erleichtert werden. Anwendungsfelder sollen insbesondere die wissenschaftliche Forschung, Gesundheitsfürsorge, Bekämpfung des Klimawandels oder Verbesserung der Mobilität sein. Der DGA kennt drei Arten der Datenintermediation – neben der Privilegierung von Datenverfügungen durch öffentliche Stellen soll auch die Errichtung vertrauenswürdiger, kommerzieller Datenintermediäre gefördert werden, sowie auch der „Datenaltruismus“ durch Spenden an Datentreuhänder. Zentral für die Datenweitergabe durch Private Intermediäre sind materielle Anforderungen an Pseudonymisierung, Anonymisierung und Interessenwahrnehmung

der betroffene Personen insbesondere, insbesondere durch sog. „Personal Information Management Services“ (PIMS). Der Gedanke, in anonymen Marktverhältnissen Transaktionen durch Errichtung von institutionellem Vertrauen zu erleichtern ist richtig. Ob freilich durch diese segmentiellen Öffnungen das Potential von Big Data hinreichend entfaltet wird, ist fraglich, zumal die privaten Empfängerorganismen ein sehr aufwändiges Zertifizierungs- und Aufsichtsprogramm absolvieren müssen.Auch öffentliche Stellen, die eine Weiterverwendung erlauben, müssen technisch angemessen ausgestattet sein, um die Vorgaben insbesondere der DSGVO und auch der Geschäftsgeheimnisrichtlinie zu gewährleisten. Problematisch ist hierbei insbesondere, welchen Anforderungen die Zustimmung zur Weiterverarbeitung personenbezogener Daten unterliegt, da der Data Governance Act ausdrücklich die Vorgaben der DSGVO unberührt lassen will (Erwägungsgrund 3) und daher insbesondere das Bestimmtheitserfordernis aus Art. 5 DSGVO fortgilt - es ist also völlig unklar, ob eine Zustimmung zur Weiterverarbeitung durch unbekannte Dritte überhaupt möglich ist, und welchen Anforderungen die Erteilung einer Vollmacht für Verhandlungen mit Dritten unterliegt, was das gesamte Konzept der Datenintermediation in Frage stellt.

II. Datenzugang unter dem Data Act

Die Europäische Kommission hat im Februar 2022 den Data Act (DA) als „letzten horizontalen Baustein der Datenstrategie“ vorgestellt; er betrifft die Frage nach den Nutzungs- und Zugangsbefugnissen für in der EU erzeugte Daten aller Art, wobei ein syntaktisches Datenverständnis zu Grunde gelegt wird, es also um die elektronische Speicherform von Information geht, nicht allerdings um die Informationsinhalte oder ihre sachliche Verkörperung. Wird der Kreis der Zugangsberechtigten erweitert, so kann auch dies „Big Data“ fördern.

Ein Zugangsrecht wird freilich nicht allgemein geschaffen, sondern es ist abhängig von vertraglichen Verhältnissen im Dreieck zwischen Nutzer, Dateninhaber und Datenempfänger – Gerätenutzer sollen Zugang zu den durch vernetzte Geräte bei der Nutzung erhobenen Daten erlangen (Art. 3, 4 DA), so dass sie ihre eigene Nutzung optimieren können und auch Dritte mit gerätebezogenen Dienstleistungen beauftragen können. Damit sind insbesondere Datenverarbeitungen im IoT-Bereich erfasst. Der Data Act regelt teils sehr detailliert die Vertragsbedingungen für die Datennutzungen in den verschiedenen Rechtsbeziehungen, dies insbesondere auch zwischen Unternehmern, um Marktmachtmissbrauch entgegenzuwirken. Bedauerlicherweise sind die Vorgaben nach allen Seiten geprägt von unbestimmten Rechtsbegriffen. Insbesondere müssen Dateninhaber Daten gegenüber dritten Datenempfängern zu FRAND-Bedin-

gungen („*fair, reasonable and non-discriminatory*“) lizensieren. Auch wirft der Data Act Probleme im Zusammenspiel mit der DSGVO auf, deren Tatbestände uneingeschränkt gelten; hingegen werden die Rechte des Datenbankherstellers eingeschränkt. Bemerkenswert ist auch, dass der Dateninhaber die vom Nutzer erhobenen Daten nach Art. 34 Abs. VI 2 DA nur auf Grund einer Lizenz wirtschaftlich verwerten darf. Allerdings könnte die Komplexität der vertraglichen Anforderungen an die Datennutzung sogar im schlimmsten Fall dazu führen, dass Datenerhebungen und Weitergaben gänzlich unterbleiben. Hier kann perspektivisch freilich die Entwicklung von Mustervertragsklauseln entgegenwirken, wie sie auch im DA vorgesehen ist.

E. Datensouveränität als Prüfstein?

Die festgestellten Defizite im europäischen System des Datenwirtschaftsrechts werfen die Frage nach einem tieferen Grund oder Rechtfertigung auf – diese lassen sich nicht allerdings gerade nicht im Streben er EU nach einer digitalen Souveränität finden.

I. Politisches Konzept digitaler Souveränität

Das Konzept der "digitalen Souveränität" hat sich in den letzten Jahren zu einem Schlüssel- und Reizbegriff in der (rechts)politischen Debatte zur Digitalisierung entwickelt. Nicht zuletzt das Erstarken autoritärer Länder wie China und Russland im digitalen Raum, allerdings auch die marktwirtschaftliche Dominanz von US-Unternehmen und der NSA-Skandal, haben zum politischen Bestreben der EU und ihrer Mitgliedstaaten nach Unabhängigkeit ihrer Bürger, Unternehmen und Regierungen im digitalen Raum geführt. Die DSGVO ist dabei fraglos das wichtigste Element. Der Begriff digitaler Souveränität ist dabei freilich sehr wertungsoffen und verschiedenartig belastbar.

Souveränität ist ein kollektivbezügliches, staatsrechtliches Konzept, welches durch verschiedene politische Ordnungen beansprucht werden kann und insbesondere im Zeitalter des Absolutismus eine zweifelhafte Prominenz erlangte, jedenfalls in demokratischen Gesellschaften das Selbstbestimmungsrecht bedeutet. Neu an der Transposition des Souveränitätskonzepts in den digitalen Raum ist, dass damit eine Aufgabe der traditionellen territorialen Bindung erfolgt. Die Nähe zu einer protektionistischen, an Autarkie orientierten Wirtschaftspolitik liegt auf der Hand.

II. Datensouveränität

Ebenso wie die Digitale Souveränität ist die Datensouveränität ein weit auslegbarer Begriff, der ganz verschiedene Aspekte individueller oder gesellschaftlicher Befähigung zum selbstbestimmten Verhalten in der Datenökonomie betrifft. Die Datensouveränität soll insbesondere die Selbstbestimmung über ausländische Datenverarbeitung bezeichnen; anders als bei der grundrechtlich verbürgten informationellen Selbstbestimmung steht freilich nicht der Abwehraspekt im Vordergrund, sondern stärker der Ermöglichungsaspekt. Im Diskurs vorzufinden ist insbesondere der Gedanke, Daten vor allem als *kollektives Gut* anzuerkennen, um Big Data zu ermöglichen, was konsequenterweise Kritik seitens Datenschützern hervorruft.

III. Keine rechtliche Bedeutung der Datensouveränität

Nach der soeben dargelegten Begriffsgenealogie ist Datensouveränität als Teilbereich Digitaler Souveränität ein unscharfer Diskursbegriff – wie die Digitale Souveränität bleibt Datensouveränität eine normative Projektionsfläche, die denkbar viel Deutungsspielraum zulässt, insbesondere da die Interessen der EU und der Mitgliedstaaten bereichsweise deutlich verschieden sind.

Damit fällt es konzeptionell durchaus schwer, die Defizite der bestehenden Datenordnung rechtlich *pauschal* durch eine Verwirklichung der Datensouveränität zu rechtfertigen. Hier fehlt es schon an der allgemein rechtsstaatlich vorausgesetzten Vorhersehbarkeit und Sicherheit des Regelungsgehalts, zumal erhebliche Sanktionsandrohungen im Raum stehen.

F. Fazit: Fokus zurück auf die dezentrale Ordnung!

Es steht damit der Befund, dass die Datensouveränität, als Teilmenge der Digitalen Souveränität, als rechtspolitisches Postulat eine ernste Herausforderung – wenn nicht gar eine Gefahr – für die Prinzipien der Europäischen Binnenordnung ist. Die wirtschaftspolitisch motivierte Kontrolle und Kommodifizierung von Datentransaktionen fußt richtigerweise auf einer dezentralen Entscheidungsprärogative der Datensubjekte; indes sind zugleich die Funktionsbedingungen der errichteten Schutzordnung – zumindest im hier beleuchteten Bereich personenbezogener Daten – nicht auf Transaktionseffizienz oder die Verwirklichung informationeller Selbstbestimmung ausgerichtet. Es scheint freilich gerade nicht angemessen, diese Güter einem vagen Konzept von Digitaler Souveränität zu opfern, selbst wenn diese faktisch Ziel der Regulierung des europäischen Datenbinnenmarktes ist.

Vielmehr wäre es konsequent die Entscheidungsmacht der Datensubjekte zu stärken, um damit mittelbar auch die Souveränität des als kollektiv gedachten Binnenmarktes zu stärken. Dieser mittelbare Ansatz muss zentral für die künftige Ordnung des Binnenmarktes für Daten sein.

*