Digitale Autonomie in Vertragsbeziehungen

Martin Nettesheim 2022-10-12T10:59:09

I. Meinungsverschiedenheiten zweier Generalanwälte

Es kommt selten vor, dass zwischen zwei Generalanwälten des Europäischen Gerichtshofs bei der Interpretation eines grundlegenden Rechtsakts der Europäischen Union (EU) grundsätzliche Deutungsunterschiede aufbrechen. Dies ist dieser Tage hinsichtlich der Datenschutz-Grundverordnung (DSGVO) geschehen.

Im Verfahren „Meta Platforms Inc. u.a./Bundeskartellamt“ (Rs. C-252/21) geht es unter anderem um die Frage, auf welche Rechtfertigungsgründe sich ein Unternehmen der Digitalwirtschaft stützen kann, wenn es Daten der Vertragspartnerinnen verarbeitet. Art. 6 Abs. 1 DSGVO stellt die Verarbeitung persönlicher Daten unter einen Rechtfertigungsvorbehalt und sieht unter anderem die Einwilligung (lit. a)), die Erforderlichkeit zur Vertragsdurchführung (lit. b)) und berechtigte Interessen (lit. f)) vor.

Generalanwalt *Rantos* hat sich in seinen Schlussanträgen vom 20. September 2022 einer im datenschutzrechtlichen Schrifttum verbreiteten Sichtweise angeschlossen, wonach den Rechtfertigungsgründen der lit. b) und lit. f) möglichst wenig Raum eröffnet werden dürfe, um dem Einwilligungsrecht des lit. a) einen möglichst weiten Anwendungsbereich zu eröffnen (Rdnr. 53-65). Sein Verständnis des Art. 6 Abs. 1 DSGVO zielt darauf ab, die spezifische Kontrollmöglichkeit der Datensubjekte über „ihre“ Daten zu stärken, die sich mit der frei erteilbaren und jederzeit widerrufbaren Einwilligung nach lit. a) verbindet. Es geht ihm damit darum, den von einer Verarbeitung betroffenen Betroffenen willkürliche Entscheidungsfreiheit zu eröffnen. Das in Art. 1 Abs. 1 DSGVO angesprochene Ziel des freien Verkehrs von Daten spielt in seinen Überlegungen keine Rolle; die Bestimmung wird nicht erwähnt. Auch das allgemeinere Ziel der EU, zur Stärkung der europäischen Wettbewerbsfähigkeit und zur Sicherung des Wohlstandsniveaus der europäischen Bevölkerung funktionierende Datenmärkte zu errichten, spielt für ihn keine Rolle.

Einen entgegengesetzten Standpunkt nimmt Generalanwalt *Campos Sánches-Bordona* in Schlussanträgen vom 6. Oktober 2022 (Rs. C-300/21, UI/Österreichische Post AG) ein. Der Generalanwalt räumt zwar ein, dass die Einwilligung des Datensubjekts „als maximaler Ausdruck von Kontrolle“ anzusehen sei (Rdnr. 73). Er schließt daran dann aber die Feststellung an: „Meines Erachtens lässt sich aus der DSGVO nicht ohne Weiteres ableiten, dass sie der betroffenen Person die Kontrolle über personenbezogene Daten als Wert an sich verleihen soll. Und ebenso wenig, dass die betroffene Person die *größtmögliche Kontrolle* über diese Daten

ausüben soll“ (Rdnr. 74). Er weist darauf hin, dass es nicht auf der Hand läge, dass die Kontrolle über die Daten zum Wesensgehalt des Grundrechts nach Art. 8 GRCh gehöre. Im Gesetzgebungsverfahren der DSGVO sei vorgeschlagen worden, einen Erwägungsgrund aufzunehmen, der das Recht der Datensubjekte ansprach, „die Kontrolle über die verarbeiteten personenbezogenen Daten auszuüben“; dieser Vorschlag sei aber gerade nicht realisiert worden. Wie weit die Rechtsauffassung der beiden Generalanwälte voneinander abweicht, wird deutlich, wenn man sich vor Augen hält, dass Generalanwalt *Campos Sánches-Bordona* das Ziel der DSGVO, den freien Datenverkehr zu fördern, explizit erwähnt (Rdnr. 58) und dann feststellt: „Die Stärkung der Kontrolle des Bürgers über die seine Person betreffenden Informationen im digitalen Umfeld gehört zu den anerkannten Zielen der Modernisierung der Regelung zum Schutz personenbezogener Daten (gehöre), ist aber kein unabhängiges oder isoliertes Ziel.“ (Rdnr. 79. Das Ziel sei vielmehr im Zusammenhang mit dem Anliegen zu lesen, „das Potential der digitalen Wirtschaft auszuschöpfen sowie ‚Wirtschaftswachstum und Wettbewerbsfähigkeit der EU‘ zu steigern.“ (Rdnr. 80).

Im Kontrast der beiden Schlussanträge treten deutlich unterschiedliche Datenschutzphilosophien zutage. Die Beobachtung derartiger Divergenzen ist nicht nur von akademischem Interesse. Die Art, wie man sich positioniert, schlägt sich unmittelbar auf die Auslegung sowohl des Art. 8 Abs. 1 GRCh und auf die Auslegung von Art. 6 Abs. 1 DSGVO nieder. Die Diskussion darüber, wie Datenschutz in der modernen Digitalgesellschaft zu verstehen ist, ist bislang nicht deutlich über Positionen hinweggekommen, wie sie in Zeiten der vorwiegend staatlichen Datenverarbeitung im längst vergangenen 20. Jahrhundert entwickelt wurden.

Im Folgenden soll begründet werden, dass das von Generalanwalt *Campos Sánches-Bordona* entwickelte Verständnis von datenschutzrechtlicher Autonomie gegenüber dem von Generalanwalt *Rantos* vertretenen Ansatz deutlich vorzugswürdig ist (nachfolgend II.). Hieraus ergeben sich dann Folgerungen für das Verhältnis von Datenschutzrecht und Privatautonomie (nachfolgend III.) und für die Auslegung von Art. 6 Abs. 1 DSGVO (nachfolgend IV.). Der Beitrag schließt mit dem Hinweis darauf, die Notwendigkeit der Sicherung der digitalen Wettbewerbsfähigkeit der EU nicht aus dem Blick zu verlieren (nachfolgend V.).

II. Digitale Autonomie als Willkür oder als Gestaltung

Die EU hat mit dem Erlass der DSGVO die Grundlagen dafür gelegt, dass das in Art. 8 Abs. 1 GRCh grundrechtlich garantierte digitale Schutzniveau etabliert und gewahrt wird. Die Herausforderung ist, die – in vielerlei Hinsicht offenen und konkretisierungsbedürftigen – Bestimmungen der DSGVO so zu interpretieren, dass das Ziel der digitalen Autonomie auch tatsächlich in der Lebenswelt realisiert wird. Dabei geht es nicht zuletzt darum, welcher Raum Verträgen eingeräumt wird, deren Gegenstand digitale Leistungen bilden. Datenschutzrechtliche Fragen stellen sich, wenn diese Leistungen unter Rückgriff auf persönliche Informationen des Vertragspartners erstellt werden. Wie soll man sich derartigen Vertragsbeziehungen

nähern? Hier lassen sich zwei Grundauffassungen bzw. Schutzphilosophien gegenüberstellen.

Digitale Autonomie als willkürliche „Kontrolle“

Im Zentrum der einen, sicherlich älteren Schutzphilosophie steht die Auffassung, dass digitale Autonomie im Kern darin bestehe, die Möglichkeit einer dauerhaften Kontrolle über die „eigenen“ persönlichen Daten haben. Digitale Autonomie wird im Kern dadurch hergestellt, dass die Menschen in jede Form der Verarbeitung „ihrer“ Daten einwilligen müssen und die Einwilligung auch jederzeit widerrufen können. Es ist dies eine Datenschutzphilosophie, die ihre Wurzeln in den 1970er Jahren hat und damals für das Verhältnis von Staat und Bürger entwickelt wurde. Sie wird nunmehr auf die Verhältnisse in der Digitalgesellschaft erstreckt. Kontrolle bedeutet danach, die Entscheidung darüber zu behalten, ob man in Wirtschaft, Kultur und Gesellschaft als Person überhaupt digital in Erscheinung tritt, zudem, mit welchen persönlichen Informationen dies geschieht. Wichtig ist hier, dass diese Philosophie nunmehr auch in Vertragsbeziehungen in der Digitalwirtschaft zum Tragen kommen soll. Regelmäßig wird damit das regulatorische Ideal verbunden, dass die Verbreitung persönlicher Daten minimiert werden sollte. Dieser Auffassung zufolge muss es darum gehen, den Anwendungsbereich von Art. 6 Abs. 1 lit. a) DSGVO (datenschutzrechtliche Einwilligung) auch in Vertragsbeziehungen möglichst weit auszudehnen. Das bedeutet zugleich, dass der Anwendungsbereich anderer Rechtfertigungsgründe, vor allem von Art. 6 Abs. 1 lit. b) DSGVO, restriktiv verstanden werden muss.

Digitale Autonomie als Gestaltungsrecht in Sozialbeziehungen

Auf der anderen Seite steht eine Schutzphilosophie, die das Ideal digitaler Autonomie nicht vorrangig in der Kontrollmacht über digitale persönliche Information in öffentlichen Räumen erblickt. Diesem Verständnis zufolge bedeutet digitale Autonomie zunächst und vor allem, auf den Gebrauch persönlicher Informationen durch Dritte gestaltend Einfluss nehmen zu können. Wer digitale Autonomie stärken will, wird dieser Sichtweise zufolge vor allem darauf hinwirken, die Rechtsmacht der Menschen zu effektivieren, in den von ihnen gepflegten wirtschaftlichen und sozialen Beziehungen darüber mitzubestimmen, wie persönliche Informationen genutzt werden. Wie weit dies gehen muss, ist kontextabhängig. Für den hier interessierenden *Bereich der Verträge mit digitalem Inhalt* kommt es vor allem darauf an, dass die Menschen (als Vertragspartner und Datensubjekte) in die Lage versetzt werden, eine faire und angemessene vertragliche Bindung eingehen und in diesem Kontext über die Nutzung ihrer Daten bestimmen zu können. Digitale Autonomie umfasst dieser Sichtweise zufolge auch die Freiheit, über die persönlichen Daten als Gut mit Marktwert zu verfügen. Autonomie lässt sich nicht auf die (missverständlich so bezeichnete) persönlichkeitsrechtliche Dimension der digitalen Identität reduzieren, sondern erstreckt sich auch auf die ökonomische Dimension. Wer den Menschen digitale Autonomie im Markt absprechen will, stärkt dieser Sichtweise zufolge nicht die Selbstbestimmung, sondern beschneidet sie paternalistisch.

Die letztgenannte Schutzphilosophie stellt das Recht der Menschen ins Zentrum, in vertragliche Rechtsbeziehungen einzutreten (oder dies zu unterlassen), in denen (auch) die Verwendung persönlicher Informationen zum gegenseitigen Vorteil geregelt wird. Die digitale Autonomie umfasst nach dieser Auffassung auch die Freiheit, über personenbezogene Daten als einem Wirtschaftsgut mit Marktwert zu verfügen. Es ist kein Verlust, sondern ein Gewinn an Autonomie, wenn ein Datensubjekt einem Dritten das vertragliche Recht einräumt, persönliche Informationen zu verwenden, deren Verarbeitung erforderlich ist, um eine erwünschte Dienstleistung zu erhalten (vorbehaltlich angemessener Einschränkungen, z. B. in Bezug auf die Datensicherheit, die Zweckbindung, angemessene Aufbewahrungsfristen und ihre anderen Rechte, z. B. im Rahmen der DSGVO). In diesem Fall bedeutet Selbstbestimmung, einzusehen, dass der Erwerb einer Dienstleistung, die die Verarbeitung von Daten erfordert, einen Wert hat. Die datenschutzrechtliche Respektierung der Privatautonomie des Datensubjekts schützt Selbstbestimmung; wer auf ein willkürliches Einwilligungsrecht setzt, stellt die Privatautonomie statt dessen in Frage.

Ausdruck des Gebrauchs wahrer digitaler Autonomie ist danach nicht die isolierende (und das Individuum atomisierende) Verweigerung der Einwilligung zur Verwendung persönlicher Daten, sondern die immer sozial integrierende privatautonome Vereinbarung mit Dritten darüber, ob und wie die verfügbaren persönlichen Informationen verwandt werden können. Natürlich umschließt dies auch die Freiheit, keine diesbezüglichen Vereinbarungen einzugehen und so den Gebrauch zu verhindern. Dies ist dann aber nur eine von vielen Optionen – und nicht das Leitziel der Idee digitaler Autonomie.

Der zuletzt beschriebenen Sichtweise zufolge stehen Art. 6 Abs. 1 lit. b) und Art. 6 Abs. 1 lit. a) DSGVG normativ jedenfalls gleichberechtigt nebeneinander. Dort, wo eine wirksame Absprache über die Verwendung von Daten getroffen wurde, hat sich Autonomie manifestiert; es besteht kein Anlass, hier noch auf Leistungserbringungsebene ein Einwilligungserfordernis nachzuschalten. Dieser Sichtweise zufolge kommt dem Datenvertragsrecht (unter Einschluss eines digitalen Verbraucherschutzrechts) bei der Realisierung des in Art. 8 Abs. 1 GRCh avisierten Schutzniveaus eine zentrale und vorrangige Bedeutung zu. Das Einwilligungserfordernis des Art. 6 Abs. 1 lit. a) DSGVO muss vor allem dort zum Tragen gebracht werden, wo es an vertraglichen Vereinbarungen, in denen sich die Autonomie des Datensubjekts ausdrückt, fehlt, also vor allem bei dem Zugriff auf persönliche Daten durch Dritte, die nicht in einer vertraglichen Beziehung zum Datensubjekt stehen.

Notwendigkeit der Auseinandersetzung mit dem eigenen Vorverständnis

Rechtstexte regeln den Sinnhorizont und die Vorverständnisse, die ihre Interpretation und Anwendung anleiten, regelmäßig nicht. Dies gilt auch für die DSGVO. Beide vorstehend kontrastierte Konzeptionen digitaler Autonomie lassen sich der Interpretation und Anwendung der DSGVO zugrundelegen. Die Entscheidung für eine der Konzeptionen (bzw. für Zwischenkonstrukte) determiniert allerdings regelmäßig das Interpretationsergebnis. Man sollte seine Präferenz für eine der beiden Konzeptionen (oder für eine Kombination) jedenfalls

aufdecken; bestenfalls wird sie sogar reflexiv begründet und kritisiert. Diesem Postulat ist Generalanwalt *Rantos* in den Schlussanträgen vom 20. September 2022 (Rechtssache C-252/21) nicht nachgekommen; er hat sich begründungslos der erstgenannten Sichtweise bedient. Eine Begründung für die These, dass der Anwendungsbereich von Art. 6 Abs. 1 lit. b) DSGVO möglichst restriktiv gehandhabt werden müsse, um datenschutzrechtliche Autonomie über Art. 6 Abs. 1 lit. a) DSGVO zu ermöglichen, findet sich in den Schlussanträgen nicht. Mehrfach wird auf eine Stellungnahme des European Data Protection Board (EDPB) Bezug genommen. Wer diese Stellungnahme aufmerksam liest, muss zur Kenntnis nehmen, dass ein auf Kontrolle abzielendes Datenschutzphilosophie auch dort begründungslos behauptet, nicht aber mit Argumenten unterlegt wird.

Es ist nicht sicher, ob der Generalanwalt sieht, dass er sich eines spezifischen Vorverständnisses bei der Annäherung an Art. 6 Abs. 1 DSGVO bedient, das seinerseits diskussionsbedürftig ist. Wichtiger ist, dass der vom Generalanwalt entwickelte Ansatz der je eigenständigen normativen Funktion von Art. 6 Abs. 1 b) DSGVO und Art. 6 Abs. 1 lit. a) DSGVO nicht gerecht wird. Die Bemühungen um Marginalisierung von Art. 6 Abs. 1 lit. b) DSGVO sind datenschutztheoretisch und datenschutzrechtlich verfehlt.

III. Datenschutzrecht und Privatautonomie

Notwendigkeit der Betrachtung verschiedener „choice architectures“

Die Zuordnung und Abgrenzung von Art. 6 Abs. 1 lit. a) DSGVO und Art. 6 Abs. 1 lit. b) DSGVO ist letztlich eine Bewertung verschiedener „choice architectures“. Beide Bestimmungen gewähren dem Datensubjekt Entscheidungsmacht. Wer sich für Art. 6 Abs. 1 lit. a) DSGVO als datenschutzrechtlich primären Rechtfertigungsgrund der Datenverarbeitung stark macht, denkt letztlich von der Willkürfreiheit des Menschen her. Wird in einer Vertragsbeziehung zwischen dem Unternehmen und seinen Vertragspartnern Art. 6 Abs. 1 lit. a) DSGVO zur Anwendung gebracht, bedeutet dies konkret, dass der Vertrag nur den Hintergrund für das tatsächliche Leistungs- bzw. Gegenleistungsgeschehen bildet. Die praktische Wirksamkeit hängt letztlich nicht (nur) vom Vertragswillen ab, sondern wird von einer nachgelagerten Willkürentscheidung des Datensubjekts. Das Unternehmen ist gezwungen, im Prozess der Leistungserbringung in Rechnung zu stellen, ob die Einwilligung in die Verwendung persönlicher Daten erteilt oder verweigert wurde, zudem, ob sie widerrufen wurde oder mit einem Widerruf zu rechnen ist.

Ohne Zweifel gewinnt das Datensubjekt dadurch Einfluss auf die zu erbringende Leistung. Das Unternehmen scheint gezwungen zu werden, die Leistung für das jeweilige Datensubjekt zu individualisieren. Der Prozess der Leitungserbringung in der Vertragsbeziehung wird dynamisiert und wird über die Zeit unsicher, weil die Einwilligung jederzeit widerrufen werden kann. Was konkret angeboten werden kann, wird fluide und vom Willen des Datensubjekts abhängig. Hierin liegt ohne Zweifel eine Ermächtigung des Datensubjekts, die als Autonomiegewinn gedeutet werden kann. Bislang ist nicht hinreichend darüber nachgedacht worden, ob es wirklich sinnvoll ist, in digitalen Vertragsbeziehungen durch Begründung eines

nachgeschalteten Willkürrechte eine kontinuierliche Beeinträchtigung der von Art. 16 GRC geschützten Rechtsbeziehungen hinzunehmen.

Willkür als verarmte Konzeption von Autonomie

Letztlich handelt es sich aber um eine einseitige, vielleicht sogar verarmte Konzeption von Autonomie. Dies aus mehreren Gründen.

Wer Art. 6 Abs. 1 lit. b) DSGVO zurückdrängen will und in Vertragsbeziehungen auf Art. 6 Abs. 1 lit. a) DSGVO setzt, bemüht sich um Relativierung und Entwertung der vertraglichen Vereinbarung. Die zwischen dem Unternehmen und der Vertragspartnerin geschlossene Vereinbarung soll von weiteren Einwilligungsrechten überlagert werden – und zwar ungeachtet der Frage und ohne spezifische Prüfung, ob das Vereinbarte fair und angemessen ist. In der Sache wird die Vertragspartnerin damit infantilisiert – die Fähigkeit, selbst für einen fairen und angemessenen Vertragsinhalt zu sorgen und die dann vertragskonform erbrachte Leistung zu empfangen, wird der Vertragspartnerin pauschal abgesprochen.

Die DSGVO nimmt einem Unternehmen nicht die Befugnis, die angebotene Digitalleistung zu definieren. Diese Befugnis ist auch durch Art. 16 GRCh grundrechtlich abgesichert. Wenn die Erteilung der Einwilligung vertraglich zur Voraussetzung der Leistungserbringung gemacht worden ist, verschafft Art. 6 Abs. 1 lit. a) DSGVO dem Datensubjekt nicht mehr als einen Hebel, eine Beendigung des Vertragsverhältnisses herbeizuführen. Um mehr Negation und Rückkehr in den ungebundenen Zustand geht es einer auf Willkür setzenden Datenschutzphilosophie aber nicht.[1)] Man kann dies als Ausdruck digitaler Autonomie ansehen, sollte sich aber bewusst sein, dass es sich um ein spezifisches und regressives Verständnis von Autonomie handelt. Auch die Vorstellung, dass ein Vertrag, der unter geringem Einsatz persönlicher Daten durchgeführt wird, immer besser ist als ein Vertrag, der einen erweiterten Einsatz vorsieht, ist in dieser Allgemeinheit offensichtlich falsch.

Wer dem Vertragspartner und Datensubjekt ein Einwilligungsrecht im Vertragsdurchführungsprozess (Art. 6 Abs. 1 lit. a) DSGV) zuweisen will, scheint nur Gutes zu tun. Das ist aber nicht der Fall. Wer versucht, ein bestehendes digitales Vertragsverhältnis durch Zuweisung von Einwilligungsrechte zu korrigieren, bewirkt auch Nachteile. In der komplexen Landschaft moderner Digitalwirtschaften, in der fast jede Waren- oder Dienstleistungserbringung eine Datenverarbeitung erfordert oder nach sich zieht, führt das Erfordernis der Einwilligung zu jeder einzelnen Datenverarbeitung zu Ermüdung und Sorglosigkeit, die jeden vermeintlichen Gewinn an Autonomie untergräbt. Im Prozess der Vertragsverhandlungen ist es dem Datensubjekt möglich, einen Vertragsinhalt anzustreben und bindend zu vereinbaren, den das Unternehmen möglicherweise nicht offerieren würde, wenn es mit einem jederzeitigen Widerruf der Einwilligung rechnen muss. Natürlich hängt es von den konkreten Umständen des Einzelfalls ab, ob sich das Unternehmen und seine Vertragspartnerin auf einen Vertragsinhalt einigen werden, der eine für die Vertragspartnerin günstigere Leistung enthält, als dies in dem Fall wäre, dass der Vertrag auf der Grundlage von Art. 6 Abs. 1 lit. a) DSGVO durchgeführt wird. Es ist jedenfalls nicht ausgeschlossen, dass die Vertragspartnerin, das eine

bindende vertragliche Vereinbarung eingeht, die die Nutzung persönlicher Daten umfasst, eine subjektiv wertvollere Leistung erhält als in einem Fall, in dem das Unternehmen mit einem jederzeitigen Widerrufrecht rechnen muss. Entscheidend ist hier, dass die Kosten-Nutzen-Bilanz so lagen- und einzelfallabhängig, dass die Annahme unberechtigt ist, die Zuweisung von Rechten nach Art. 6 Abs. 1 lit. a) DSGVO wären immer im Interesse des Datensubjekts. Was unberücksichtigt bleibt, ist im übrigen das öffentliche Interesse an Innovation. Wenn Unternehmen für ein Szenario entwickeln müssen, in dem Nutzer ihre Zustimmung widerrufen, wird dies die Innovationsfähigkeit für datengesteuerte Produkte massiv behindern. Eine allgemeine Abgrenzung und Zuordnung von Art. 6 Abs. 1 lit. a) und lit. b) DSGVO ist auf dieser Grundlage schon gar nicht möglich.

Datenschutzrechtliche Infragestellung der Privatautonomie?

Wer einer Datenschutzphilosophie anhängt, die den Wert einer willkürlichen Kontrolle betont, ist häufig geneigt, die vorstehend entwickelte Idee freiwilliger und gleichberechtigter Gestaltung sozialer Beziehungen als unwesentlich oder irrelevant abzutun. Teilweise findet sich auch die Strategie, den Gebrauch der Privatautonomie seitens des Datensubjekts in Frage zu stellen oder zu bestreiten. Dieser Strategie hat sich Generalanwalt *Rantos* in den Schlussanträgen vom 20. September 2022 bedient. Er zieht in seinen einführenden Bemerkungen zur Auslegung von Art. 6 Abs. 1 DSGVO die Relevanz und Freiwilligkeit der vertraglichen Erklärung des Datensubjekts suggestiv in Frage: Die Verarbeitung erfolge „auf der Grundlage der allgemeinen Vertragsbedingungen, die der für die Verarbeitung Verantwortliche ohne die Einwilligung der betroffenen Person oder sogar gegen ihren Willen vorgegeben hat“ (Rdnr. 51). Er blendet auch aus, dass das digitale Verbrauchervertragsrecht gewährleistet, dass in Digitalverträgen nichts vereinbart werden kann, was zu einer unzumutbaren Belastung der Verbraucher führen würde. Die Behauptung, dass in einem wirksam geschlossenen Vertrag etwas „gegen den Willen“ der Vertragsschließenden festgelegt würde, bedient populistische Vorurteile, sollte aber in einem Rechtsdokument des Europäischen Gerichtshofs nicht auftauchen.

Das wohl wichtigste Argument gegen die von Generalanwalt *Rantos* vertretene Sichtweise führt auf die Grundlagen des westlich-liberalen Rechtsdenkens zurück. Ethik, Recht und Politik stützen sich auf das Axiom, dass sich menschliche Selbstbestimmung nicht zuletzt in frei eingegangenen, fair ausgehandelten und inhaltlich nicht unangemessenen vertraglichen Vereinbarungen ausdrückt. Hieraus ergeben sich Bindungen, es lässt sich aber auch jener Nutzen ziehen, der den subjektiven Präferenzen der Vertragspartner entspricht. Niemand käme auf die Idee, nichtdigitale Verträge um ein willkürlich zu gebrauchendes Einwilligungsrecht auf Durchführungsebene zu ergänzen. Es gibt keinen Grund, warum dies im Bereich von Verträgen mit Digitalinhalten grundsätzlich anders sein soll. Es muss ein Anliegen der EU und der EU-Mitgliedstaaten sein, sicherzustellen, dass die rechtlichen Rahmenbedingungen geschaffen werden, die erforderlich sind, um die Fairness und Angemessenheit vertraglicher Vereinbarungen mit digitalen Inhalten sicherzustellen. Der Respekt vor der digitalen Autonomie impliziert in diesem Zusammenhang, dass genügend Raum für vertragliche Gestaltungen bleiben muss, die es den Vertragspartnern ermöglichen, ihre jeweiligen Interessen in der Digitalgesellschaft

zum Ausgleich zu bringen. Paternalismus und Bevormundung müssen vermieden werden – die Vorstellungen vom guten Leben und die Lebensmodelle werden in der Digitalgesellschaft so vielfältig sein wie in der Realwelt. Die gelegentlich zu beobachtende Vorstellung, dass in digitalen Vertragsbeziehungen alles anders als in nicht-digitalen Vertragsbeziehungen sei, ist verfehlt; sie lässt sich auch datenschutzrechtlich nicht begründen. Die Fähigkeit und der Wille selbstbestimmt handelnder Menschen, bindende Verträge mit digitalen Inhalten eingehen zu können, würde letztlich in Zweifel gerückt, wenn man die Auffassung verträte, Autonomie würde auf Durchführungsebene eine willkürlich zu gebrauchende Abwendungsmöglichkeit voraussetzen. Die Menschen werden, wie oben bereits gesagt wurde, dadurch infantilisiert. Unternehmen muss die Möglichkeit erhalten bleiben, für die Sicherheit, vertraglich über Daten disponieren zu können (lit. b), mehr versprechen, als wenn eine Abwicklung über lit a) erfolgt; ein Datensubjekt, das sich hierauf einlässt, büßt nicht Autonomie ein, sondern realisiert sie.

Der relative Wert der Ermächtigung, die in der Anwendung von Art. 6 Abs. 1 lit. a) DSGVO liegt, lässt sich daher nur sinnvoll bestimmen lässt, wenn in Rechnung gestellt wird, dass vertragliche Absprachen Ausdruck des Gebrauchs digitaler Autonomie in der Digitalökonomie sein können. Wird digitale Autonomie im Wege einer vertraglichen Absprache realisiert und datenschutzrechtlich über Art. 6 Abs. 1 lit. b) DSGVO realisiert, wird den Menschen zwar der Gebrauch freier Willkür abgeschnitten. Sie werden damit aber als Rechtssubjekte ernst genommen.

Keine datenschutzrechtliche Inhaltskontrolle von Verträgen

Dies zwingt zu der Schlussfolgerung, dass das Datenschutzrecht keine Inhaltskontrolle wirksam geschlossener zivilrechtlicher Verträge leisten kann. Immer wieder ist der Versuch zu beobachten, Art. 6 Abs. 1 lit. b) DSGVO zu einem Instrument zu machen, mit dem eine Inhaltsbewertung digitaler Verträge vorgenommen werden kann, nicht zuletzt in der schon erwähnten Stellungnahme des EDPB. Auch dies macht sich in den Schlussanträgen von Generalanwalt *Rantos* bemerkbar. „Schlechte“ Verträge sind seiner Ansicht nach dadurch zu sanktionieren, dass auf Durchführungsstufe das Einwilligungserfordernis zum Tragen kommt (Rdnr. 56 mit paternalistischen Überlegungen zum Nutzenkalkül der Datensubjekte). Seinen Schlussanträgen liegt nicht nur die These zugrunde, dass die richterliche oder administrative Überprüfung der Erforderlichkeit in Art. 6 Abs. 1 lit. b) DSGVO nicht nur die Frage zum Gegenstand hat, ob die vom Unternehmen vorgenommene Verwendung sich zur *Erfüllung des vertraglich Vereinbarten* als erforderlich erweist. Er will auf der Grundlage von Art. 6 Abs. 1 lit. b) DSGVO auch eine datenschutzrechtliche Vertragsinhaltskontrolle betreiben. Eine vertragliche Vereinbarung, die nicht auf dem Prinzip der Datenminimalisierung beruht, ist danach zwar nicht zivilrechtlich unwirksam (das liegt eindeutig jenseits der Reichweite der DSGVO); sie soll aber selbst dann nicht unter Art. 6 Abs. 1 lit. b) DSGVO fallen und als Rechtfertigung für die Verarbeitung dienen, wenn beide Seiten sie als gegenseitig fair ansehen.

IV. Folgerungen für die Auslegung von Art. 6 Abs. 1 DSGVO

Hieraus ergeben sich unmittelbare Folgerungen für die Auslegung und Anwendung von Art. 6 Abs. 1 DSGVO.

Erstens wäre die Annahme offenkundig falsch, dass sich die digitale Autonomie des Menschen in Vertragsverhältnissen immer dadurch optimieren lässt, dass Art. 6 Abs. 1 lit. a) DSGVO zur Anwendung gebracht wird. Je nach Sachlage und persönlichen Präferenzen entspricht es dem Interesse eines Datensubjektes mehr, einen Vertrag zu schließen, der sich (auch) auf die Nutzung persönlicher Daten erstreckt und der nach Art. 6 Abs. 1 lit. b) DSGVO behandelt wird. Dies gilt auf jeden Fall dann, wenn das Unternehmen digitale Dienstleistungen verlässlich gestalten will, deren Inhalt vom Unternehmen und von den Vertragspartnern zum Gegenstand eines verbraucherschutzrechtlich wirksamen Vertrags gemacht worden ist. Beiden Seiten ist langfristig nicht gedient, wenn das Unternehmen jederzeit damit rechnen muss, dass Vertragspartner ihre Einwilligung widerrufen und das Unternehmen zwingen, einen anderen Dienst anzubieten, der seinen Bedürfnissen und denen der betroffenen Person nicht vollständig entspricht. Die Bemühungen, in digitalen Vertragsbeziehungen möglichst Art. 6 Abs. 1 lit. a) DSGVO zur Anwendung zu bringen, birgt die Gefahr, dass die Fähigkeit zur Innovation und Verbesserung von Diensten und Produkten behindert wird, auch wenn genau dies von einer Vertragspartei gewünscht wird.

Zweitens wäre es schlechterdings unsinnig, eine Zuordnung von Art. 6 Abs. 1 lit. b) DSGVO und Art. 6 Abs. 1 lit. a) DSGVO vorzunehmen, ohne in Rechnung zu stellen, dass das Digitalvertragsrecht der EU und der EU-Mitgliedstaaten sicherstellt, dass Digitalverträge nur wirksam geschlossen werden können, wenn (sowohl prozedural als auch inhaltlich) bestimmte Mindestvoraussetzungen hinsichtlich Informiertheit, Fairness und Gleichwertigkeit eingehalten werden. Es wäre eine myopischer Blickverengung, sich Art. 6 Abs. 1 DSGVO zu näheren, ohne in Rechnung zu stellen, dass das Digitalvertragsrecht einen Rahmen setzt, der autonomiesichernden Fairness- und Angemessenheitsvorkehrungen enthält, und dass die vertragschließenden Parteien offensichtlich je subjektiv im Vereinbarten einen hinreichenden Wert erblickt haben. Ist vertragsrechtlich sichergestellt, dass der zwischen dem Unternehmen und dem Datensubjekt abgeschlossene Vertrag transparent ist und einen fairen Austausch von Leistung und Gegenleistung vorsieht, besteht kein Anlass, dem Datensubjekt für den Abschnitt der Durchführung noch ein Einwilligungsrecht nach Art. 6 Abs. 1 lit. a) DSGVO zu gewähren. Wer hierfür eintritt, zerstört vielmehr gerade die materielle Reziprozität, deren Definition vertragsrechtlich ermöglicht und abgesichert wird. In den Überlegungen von Generalanwalt *Rantos* wird dieser Zusammenhang von Digitalvertragsrecht und Datenschutzrecht vollständig ausgeblendet.

Deshalb besteht – drittens – Anlass, Art. 6 Abs. 1 lit. b) DSGVO beim Wort zu nehmen. Die Bestimmung sieht keine datenschutzrechtliche Kontrolle des zwischen

dem Unternehmen und dem Datensubjekt geschlossenen Vertrags vor, sondern knüpft die gesetzliche Rechtfertigung allein daran, dass bei der Durchführung des Vereinbarten nicht mehr als die *hierfür* erforderlichen Daten verarbeitet werden. Es ist nicht Regelungsgegenstand von Art. 6 Abs. 1 lit. b) DSGVO, gute von schlechten Verträgen zu unterscheiden. Art. 6 Abs. 1 lit. b) DSGVO macht die gesetzliche Rechtfertigung daher auch nicht davon abhängig, dass zwischen den beiden Vertragsparteien ein Vertrag geschlossen wurde, der (nach welchen Kriterien auch immer) „gut" ist. Art. 6 Abs. 1 lit. b) DSGVO bietet keinen Ansatzpunkt, Menschen, die informiert und frei einen von ihnen für gewinnbringend eingestuften Vertrag geschlossen haben, nunmehr vor sich selbst zu schützen. Die Bestimmung verhindert, dass Daten über das vertraglich vereinbarte („erforderliche") Maß hinaus verarbeitet werden; sie sieht aber nicht vor, dass EU-Amtswalter sich das Recht der Beurteilung des Nutzenkalküls der Menschen zuschreiben. Kurz: Angemessener Datenschutz läuft nicht auf paternalistische Bevormundung hinsichtlich individueller Präferenzen hinaus. Nur am Rande sei erwähnt, dass die DSGVO ein umfassendes Schutzsystem auch dann bereitstellt, wenn der Weg über Art. 6 Abs. 1 lit. b) DSGVO gewählt wird; sie sichert die Angemessenheit der Datenverarbeitung in vielfältiger, den Anforderungen von Art. 8 GRCh entsprechender Weise.

Hieraus ergibt sich – viertens – die dogmatische Notwendigkeit, bei der Anwendung des Erforderlichkeitskriteriums in Art. 6 Abs. 1 lit. b) DSGVO drei Ebenen sauber zu unterscheiden.

1. Es ist *nicht* Gegenstand einer datenschutzrechtlichen Erforderlichkeitsprüfung, ob das Unternehmen mit seinen Vertragspartnern auch eine andere Leistung hätte vereinbaren *können*, ebensowenig, ob das Unternehmen eine andere Leistung früher erbracht hat. Die in Art. 6 Abs. 1 lit. b) DSGVO vorgesehene Erforderlichkeitskontrolle erstreckt sich insbesondere nicht auf die Frage, ob ein Unternehmen, das mit seinen Vertragspartnern einen Vertrag über personalisierte Leistungen abgeschlossen hat, vielleicht auch einen Vertrag über nicht-personalisierte Leistungen hätte abschließen können. Eine derartige Kontrolle ist rechtlich selbst dann nicht möglich, wenn sich aufzeigen ließe, dass bei der Erstellung einer nicht-personalisierten Leistung weniger persönliche Daten verwendet werden. Das Datenschutzrecht enthält keinen substanziellen Maßstab, der in dieser Frage eine sinnvoll begründete Entscheidung tragen könnte. Wer sich hier versucht, bringt nur subjektive Präferenzen zur Geltung – so etwa die Auffassung, dass nicht-personalisierte Werbung immer besser als personalisierte Werbung sei. Wenn das Datensubjekt wohlinformiert und frei den Standpunkt eingenommen hat, dass der geschlossene Vertrag seine Präferenzen abbildet, gibt es keinen Anlass, dies datenschutzrechtlich zu korrigieren. Bestehen Zweifel daran, ob ein fairer Vertrag geschlossen wurde, ist hierauf vertragsrechtlich zu reagieren.
2. Die datenschutzrechtliche Erforderlichkeitsprüfung nach Art. 6 Abs. 1 lit. b) DSGVO kann auch nicht als Hebel dienen, mit dem ein Unternehmen dazu veranlasst werden soll, im Durchführungsprozess von dem vertraglich Vereinbarten abzuweichen. Ist in dem Vertrag zwischen Unternehmen und Vertragspartnerin die Erbringung einer personalisierten Leistung vereinbart, die vertragskonform unter Rückgriff auf persönliche Informationen erstellt

werden kann, kann nicht datenschutzrechtlich argumentiert werden, dass das Unternehmen (in Abkehr vom Vertrag) auch eine andere Leistung erbringen könnte.

3. Die Erforderlichkeitsprüfung nach Art. 6 Abs. 1 lit. b) DSGVO erstreckt sich allein auf die Prüfung, ob das Unternehmen im Prozess der Leistungserbringung Daten erhebt oder verwendet, die nicht erforderlich sind, um den vertraglich vereinbarten Leistungsgegenstand zu erstellen. Diesbezüglich handelt es sich dann um einen Rechtsbegriff des Unionsrechts; und diesbezüglich kann die Entscheidung natürlich nicht dem Unternehmen überlassen bleiben, sondern muss auf „objektive“ Umstände gestützt werden. Kurzum: Wer Fragen der vertraglichen Leistungsdefinition und der Leistungserbringung durcheinander bringt, wird den rechtlichen Anforderungen an die Anwendung des Erforderlichkeitskriteriums schon im Ansatz nicht gerecht.

Aus dem Gesagten folgt fünftens, dass die rechtspolitische Annahme falsch wäre, dass dem Datensubjekt über die Anwendung von Art. 6 Abs. 1 lit. a) DSGVO ein faktisches Bestimmungsrecht über die unternehmerische Leistung verschafft werden könnte (oder gar verschafft werden müsste). Das Datenschutzrecht greift nicht in das unternehmerische Leistungsbestimmungsrecht ein. Es hat auch keinen Vorrang vor anderen Zielen der EU, etwa die Sicherung der EU-Wettbewerbsfähigkeit, der Innovationskraft der Unternehmen im EU-Binnenmarkt oder der grundrechtlichen Freiheit aus Art. 16 GRCh (DSGVO, Begründungserwägung 4). Ein Unternehmen hat die Freiheit, in den Markt mit einem Leistungsangebot einzutreten, das allein und ausschließlich personalisierte Dienstleistungen zum Gegenstand hat. Datensubjekte haben dann die Möglichkeit, das Angebot anzunehmen oder nicht. Sie haben keinen Anspruch auf Anpassung, etwa in Richtung Datenminimierung. Art. 6 Abs. 1 DSGVO enthält insbesondere keinen Hebel, mit dem Unternehmen, die eine personalisierte Dienstleistung im Markt anbieten, datenschutzrechtlich zur Umstellung auf eine nichtpersonalisierte Dienstleistung gezwungen werden könnten.

V. Grundlage der Digitalwirtschaft muss der bindende Vertrag über digitale Inhalte sein

Das EU-Datenschutzrecht steht gegenwärtig vor der Herausforderung, sich aus einer eindimensionalen Vorstellungswelt herauszulösen, wonach das Einwilligungserfordernis nach Art. 6 Abs. 1 lit. a) DSGVO die digitale Autonomie der Menschen immer optimiere. Es lässt sich unschwer aufzeigen, dass in Vertragsverhältnissen die Anwendung von Art. 6 Abs. 1 lit. a) DSGVO in dem Sinne zu einem Autonomieverlust führen kann, dass bestimmte Vereinbarungen nicht mehr getroffen werden können. Das Schutzziel von Art. 8 Abs. 1 GRCh wird sich nicht verwirklichen lassen, wenn nicht berücksichtigt wird, dass Art. 6 Abs. 1 lit. b) DSGVO und Art. 6 Abs. 1 lit. a) DSGVO je unterschiedliche „choice architectures“ zu Wege bringen. Die simplifizierende These, dass in die Rechtfertigungsgründe des Art. 6 Abs. 1 DSGVO eine normative Hierarchie eingebaut ist, an deren Spitze Art. 6 Abs. 1 lit. a) DSGVO steht, ist zurückzuweisen. Es gilt, den eigenständigen Wert von Art. 6 Abs. 1 lit. b) DSGVO zu erkennen. Waren die Verfasser der DSGVO klüger als ihre gegenwärtigen Interpreten?

Das Digitalzeitalter hat vor nunmehr zwanzig Jahren begonnen. Es scheint, als ob sich die digitale Transformation zuletzt weiter beschleunigt hat. In immer mehr Lebensbereichen zeigen sich Manifestationen des Digitalen, und immer mehr Vertragsbeziehungen erstrecken sich auf digitale Inhalte. Bislang lässt sich noch nicht einmal in vagen Umrissen erkennen, wie die künftige Digitalgesellschaft einmal aussehen wird. Die sich hieraus ergebenden rechtspolitischen Anforderungen sind enorm: Regulierung ins Blaue hinein ist ebenso untunlich wie naiver Fortschrittsglaube oder fatalistische Untätigkeit. Ein wesentliches Anliegen von Recht und Politik muss es sein, sicherzustellen, dass den Menschen auch in der sich herausbildenden Digitalgesellschaft die Führung eines selbstbestimmten und guten Lebens möglich ist. Der Weg in die digitale Zukunft darf nicht in einen Zustand führen, in dem den Menschen im digitalen Leben die autonome Selbstbestimmung abhanden gekommen ist. Zugleich müssen Recht und Politik auch im neuen – durch datenökonomische Gegebenheiten geprägten – Umfeld sicherzustellen, dass eine wettbewerbsfähige und innovationskräftige Ökonomie entsteht und erhalten bleibt. Nur Wettbewerb und Innovation können die Präferenzen der Menschen in der Digitalgesellschaft effektiv bedienen; ohne sie wird sich nicht nur das in der EU erreichte Wohlstandsniveau nicht halten lassen. Über digitale Autonomie zu sprechen, ohne die Erfordernisse einer funktionierenden Wirtschaft im Blick zu haben, ist im besten Fall myopisch, im schlechtesten sogar sinnfrei.

Generalanwalt *Campos Sánches-Bordona* hat sich in Schlussanträgen vom 6. Oktober 2022 zukunftsoffen gezeigt und die Bedeutung des Schutzes der EU-Wettbewerbsfähigkeit und der Innovationskraft betont. Er hat das Datenschutzrecht in größeren Kontext gestellt und jede myopische Betrachtungsweise vermieden. Sein Schlussantrag steht für eine zukunftsgerichtete Interpretation des Datenschutzrechtes.

Der Autor ist Inhaber des Lehrstuhls für Staats- und Verwaltungsrecht, Europarecht und Völkerrecht an der Juristischen Fakultät der Universität Tübingen. Er hat Meta Platforms Inc. (vormals Facebook Inc.) im Jahr 2019 in der Frage des Verhältnisses der Befugnisse von Datenschutzbehörden (Art. 51-66 DSGVO) und Wettbewerbsbehörden (§ 19 GWB) beraten (Vorlagefragen 1 und 7 in der Rechtssache C-252/21).

References

- Zugunsten dieser Konzeption digitaler Autonomie wird regelmäßig angeführt, dass diese Option Unternehmen dazu veranlassen wird, ihre Leistung so zu definieren und zu erbringen, dass Datensubjekte nicht vom Widerrufsrecht Gebrauch machen.
