

Jürgen Kühling, Paul M. Schwartz

Daten gegen Leistung

Konvergenz von kalifornischem Recht und DSGVO?¹

Das Modell „Daten gegen Leistung“ ist nach der DSGVO unter strengen Voraussetzungen zulässig. In den USA ist das kalifornische Datenschutzrecht Vorreiter bei der Fundierung und Einhegung dieses Ansatzes.

Mit dem Meta-Urteil hat der EuGH am amerikanischen Unabhängigkeitstag (4. Juli 2023) einen wichtigen Schritt in Richtung Bändigung der Datenverarbeitung durch Big-Tech-Unternehmen gemacht. Zugleich hat er die Grundlage für neue Strukturen bei der Bezahlung von Leistungen – wie der Nutzung von Social-Media-Plattformen – mit Daten geschaffen. Weitgehend unbeachtet von den Diskussionen in der wissenschaftlichen Literatur in Europa zeichnet sich im Datenschutzrecht Kaliforniens – dem Sitz zahlreicher global digitaler Player wie Meta – eine vergleichbare Entwicklung ab (dazu 1), die sich als inspirierend für den europäischen Diskurs erweisen kann (dazu 4). Das gilt nicht zuletzt deshalb, weil der kalifornische Ansatz schon einer spannenden und facettenreichen wissenschaftlichen Kritik in der US-amerikanischen Literatur ausgesetzt ist (dazu 2) und daher bei der Analyse der konvergierenden Rechtssituation in der EU (dazu 3) fruchtbar gemacht werden kann.

1 Daten gegen Leistung in Kalifornien

Kalifornien war der erste Bundesstaat in den USA, der in den Jahren 2018 und 2020 ein umfassendes Datenschutzregime geschaffen hat² (1.1). Dieses Regelwerk enthält auch eine Rechtsgrundlage für die Kommerzialisierung der eigenen personenbezogenen Daten (1.2). Die Bestimmung wurde inzwischen durch eine Verordnung der neu geschaffenen kalifornischen Datenschutzaufsichtsbehörde näher konkretisiert (1.3). Dabei nimmt Kalifornien eine Vorreiterrolle im Datenschutz in den USA ein. Einzelne weitere Bundesländer folgen diesem Ansatz im Allgemeinen und der legitimierenden Steuerung des Austauschs von Daten gegen Leistungen im Besonderen (1.4).

1.1 Der kalifornische Datenschutzrahmen

Der kalifornische Datenschutzrahmen wurde zuerst mit dem California Consumer Privacy Act (CCPA; 1.1.1) geschaffen, der durch den California Privacy Rights Act (CPRA) modifiziert wurde (1.1.2). Integriert wurden die neuen Regeln in das kalifornische Zivilgesetzbuch (Cal. Civ. Code, § 1798.100 ff.; im Folgenden ohne weiteren Zusatz zitiert). Dadurch wird zwar kein vollständig spezifisch ausgeformtes Datenschutzregime etwa mit einer eigenständigen Definition aller beteiligten Akteure (wie „betroffene Personen“ in der DSGVO) und relevanten Güter geschaffen. Gleichwohl werden die zivilrechtlichen Bestimmungen entsprechend umfassend ergänzt – auch mit einzelnen spezifischen Definitionen. Objektiver Schutzgegenstand sind so „personal information“, die definiert werden als Informationen, die auf Konsumenten oder Haushalte³



Prof. Dr. Jürgen Kühling, LL.M.,

ist Inhaber eines Lehrstuhls für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht an der Universität Regensburg. Seit September 2020 ist er Vorsitzender der Monopolkommission.

E-Mail: Juergen.Kuehling@jura.uni-regensburg.de



Prof. Paul M. Schwartz, J.D.,

ist Jefferson E. Peyser Professor an der Universität Kalifornien, Berkeley Law School und Mitglied des Direktoriums des Berkeley Center for Law & Technology.

© Der/die Autor(en) 2023. Dieser Artikel ist eine Open-Access-Publikation.

¹ Gefördert durch die Deutsche Forschungsgemeinschaft (DFG), Projektnummer 463332313. Der Beitrag ist während eines von der DFG geförderten Forschungsaufenthalts des Autors Kühling im September 2022 vorbereitet und im September 2023 vor Ort in Zusammenarbeit mit dem kalifornischen Kollegen Schwartz abgeschlossen worden. Die Autoren danken der Kollegin Jennifer M. Urban, Juraprofessorin der UC Berkeley und erste Vorsitzende der kalifornischen Datenschutzaufsichtsbehörde, sowie zahlreichen weiteren Kolleginnen und Kollegen wie Jenniger King (Stanford) und Eric Goldmann (Santa Clara) für anregende Gespräche. Ferner dankt Kühling seinem Lehrstuhlteam, insbesondere Carolin Losch und Cajetan Späth, für die Unterstützung bei der Recherche vor Ort.

² Schwartz/Solove, *Information Privacy Law*, 7. Aufl. 2021, 970-973.

³ Die eigenständige Erfassung auch von Haushalten ist besonders interessant, da es auch eine ganze Reihe relevanter Fälle von Haushaltsdaten gibt, die einem Modell von Daten gegen Leistung folgen können, etwa die Energie- oder Telekommunikationsdaten von Haushalten; zur Erfassung von Haushaltsdaten

bezogen werden können, § 1798.140(v)(1). Nicht geschützt werden öffentlich verfügbare Informationen und aggregierte Konsumenteninformationen. Sodann werden bestimmte Bereiche durch spezifischere Regeln gesteuert, etwa Patientenakten oder Kreditinformationen, § 1798.145(c)(d)(e)(g). Der subjektiv geschützte Kreis der Konsumenten erfasst nur natürliche Personen mit Wohnsitz in Kalifornien, § 1798.140(i). Verpflichtete sind zunächst die Unternehmen, die mit Profitorientierung (§ 1798.140(d)(1)) die Daten von den Konsumenten erheben, sodann aber auch die von diesen eingeschalteten Diensteanbieter und Vertragspartner sowie sonstige Dritte, die Zugang zu den Konsumentendaten erhalten. Dies gilt im Übrigen auch für Unternehmen aus anderen Bundesstaaten der USA genauso wie für europäische und damit auch deutsche Unternehmen, die Daten kalifornischer Konsumenten verarbeiten.⁴

1.1.1 California Consumer Privacy Act, CCPA

Der CCPA wurde am 28. Juni 2018 verabschiedet und trat am 1. Januar 2020 in Kraft. Er wird begleitet durch Regelungen des kalifornischen Attorney General (Generalstaatsanwalt)⁵, der auch für den Vollzug des CCPA zuständig ist. Normativer Ausgangspunkt ist im Übrigen nicht wie in der DSGVO ein Verbot mit Zulässigkeitsstatbeständen⁶, sondern – als vorliegend zentrale materiell-rechtliche Regelungen – ein Opt-out-Recht der Konsumenten (§ 1798.120(a)) und ein Recht auf diskriminierungsfreie Behandlung (§ 1798.125(a)). Zudem werden vergleichbar dem Ansatz in der DSGVO eine Reihe von prozeduralen und prozesualen Konsumentenrechten geschaffen wie Auskunftsrechte (§ 1798.110), Löschansprüche (§ 1798.105) und Klagerechte bei Datenschutzverletzungen (§ 1798.150). Notwendig ist dabei ein Sammeln (§ 1798.140(f)) oder Verkaufen (§ 1798.140(ad)) von Daten, wobei die jeweiligen Tatbestände weit gefasst sind – ähnlich weit wie der Begriff der Datenverarbeitung nach der DSGVO. So geht es insbesondere nicht nur um das Verkaufen von Daten an Dritte, sondern etwa auch um die Weitergabe im eigenen Konzernverbund, was für Unternehmen wie Meta von großer Bedeutung ist.

1.1.2 California Privacy Rights Act, CPRA

Der CPRA ändert wiederum den CCPA. Ziel des CPRA ist es, freiwillige und vernünftige Entscheidungen der Konsumenten in Bezug auf die Verarbeitung der sie betreffenden Daten durch Unternehmen zu gewährleisten. Vorangetrieben wurde diese deutliche Verschärfung und Erweiterung des Datenschutzregimes durch ein Volksbegehren, das in der kalifornischen Verfassung vorgesehen ist (Article II, Section 9⁷). Dabei wurde der

CPRA im Jahr 2020 vom kalifornischen Wahlvolk als Proposition 24 angenommen und trat am 16. Dezember 2020 in Kraft, allerdings mit einer Übergangszeit für die wesentlichen Vorschriften bis zum 1. Januar 2023. Die Durchsetzung erfolgt durch eine eigens geschaffene Datenschutzaufsichtsbehörde, die California Privacy Protection Agency (CPPA). Auch dies ist ein Novum in den USA.⁸ Die CPPA entscheidet durch ein Board mit fünf Mitgliedern, die über eine heterogene aber insgesamt umfassende Erfahrung in der Verwaltung, der Wissenschaft und bei der Durchsetzung von Datenschutzfragen verfügen. Jennifer M. Urban, eine Juraprofessorin der UC Berkeley, ist die erste Vorsitzende (Chair) des Gremiums. Die Durchsetzungsbefugnisse wurden zum 1. Juli 2023 „scharf gestellt“, § 1798.185(d). Eine klärende Anwendungspraxis wird also jetzt erst zu erwarten sein.

Damit sind zwei Behörden mit unterschiedlicher Stoßrichtung für den Datenschutz gegenüber Unternehmen zuständig, da die Kompetenzen des Generalstaatsanwalts unberührt bleiben, § 1798.199.90. Allerdings wird der Generalstaatsanwalt nicht tätig in Fällen, in denen bereits die CPPA tätig geworden ist. So wird eine „Kakophonie“ der beiden Behörden verhindert. Zugleich ist angesichts des Budgets der CPPA (10 Mio. \$ gem. § 1798.199.95(a)) die Datenschutzaufsichtsbehörde auf eine Zusammenarbeit mit dem Generalstaatsanwalt angewiesen, gerade bei der gerichtlichen Durchsetzung im Falle von Datenschutzverstößen.

Inhaltlich schafft der CPRA, inspiriert u.a. durch die DSGVO⁹, neue Konsumentenrechte, namentlich einen Berichtigungsanspruch (§ 1798.106) und ein Recht, die Verarbeitung sensibler personenbezogener Daten zu beschränken (§ 1798.121). Im Übrigen wird auch das Teilen von Daten in einem weit verstandenen Sinne als Datenverarbeitungsvorgang erfasst, § 1798.140(ah). Sodann definiert § 1798.140(h) die Einwilligung durchaus mit der DSGVO vergleichbar. So kommt es auf die Freiwilligkeit, Bestimmtheit, Informiertheit sowie Klarheit des Konsumentenwillens an. Die Einwilligung ist allerdings vor allem für die Verarbeitung sensibler Daten relevant, da es im Übrigen – jedenfalls für Erwachsene¹⁰ – beim Opt-out-Modell bleibt. Immerhin sieht der CPRA aber die Möglichkeit eines „Opt-out-Präferenzsignals“ vor, § 1798.185(a)(19), das der Konsument als Voreinstellung an alle Unternehmen senden kann und dessen Regeln durch den Generalstaatsanwalt näher ausdifferenziert wurden.¹¹

1.2 § 1798.125 als Grundlage

Die wesentliche Grundlage für die Ausgestaltung des Modells „Daten gegen Leistung“ findet sich sodann in § 1798.125. Ausgangspunkt ist dabei, dass Konsumenten grundsätzlich keine preislichen oder sonstigen nicht-preislichen Nachteile dadurch erleiden dürfen, dass sie von ihrem Opt-out-Recht bei der Datenverarbeitung Gebrauch machen. Entscheidend ist dann jedoch die wichtige Ausnahme, dass eine Differenzierung sehr wohl zulässig ist, wenn diese einen „reasonably-related“-Test erfüllt, d.h.

und insbesondere dem problematischen Aspekt der Einwilligung weiter *Buchner/Kühling* in: Kühling/Buchner, DS-GVO/BDSG, 4. Aufl. 2024 (im Erscheinen), Art. 7, Rn. 18a ff. Zum kalifornischen Recht siehe den knappen Hinweis bei *Hoeren/Pinelli*, MMR 2018, 711 (712 f.).

⁴ Zu den Voraussetzungen im Überblick *Determann*, ZD 2018, 443 (444 f.).

⁵ In den USA fungiert der Attorney General auf der Bundesebene und auf der Ebene eines Bundesstaates sowohl als Generalstaatsanwalt als auch als Justizminister, siehe dazu *Haas* in: Jäger/Haas/Welz, Regierungssystem der USA, 3. Aufl. 2007, S. 459 (473); *Patrich/Pious/Ritchie*, The Oxford Guide to the United States Government, 2001, S. 35 f.

⁶ Dazu *Kühling/Klar/Sackmann*, Datenschutzrecht, 5. Aufl. 2021, Rn. 334.

⁷ Siehe dazu z. B. *Carrillo u.a.*, California Constitutional Law: Direct Democracy, Southern California Law Review 92 (2019), S. 557 ff.; *Determann*, ZD 2021, 69.

⁸ Dazu *Determann*, ZD 2021, 69 (71).

⁹ Siehe exemplarisch aus den vielen knappen Einordnungen in diese Richtung *Khoury*, California's Mini-GDPR? The Newly-Enacted California Consumer Privacy Act of 2018 (10.7.2018), <https://www.lexology.com/library/detail.aspx?g=60487525-76ea-44e3-97a8-3b9b02987c2e/> (zul. abgerufen am 25.9.2023); zu diesem „Brussels effect“ im Datenschutz allgemein *Bradford*, The Brussels Effect, 2020.

¹⁰ Zum Opt-in-Modell für Kinder § 1798.120(d), dazu wiederum *Determann*, ZD 2021, 69 (71).

¹¹ Tit. 11 § 7013 Cal. Code Regs., vormals § 999.306. Cal. Code Regs.

angemessen bzw. fair bezogen auf den Wert der Daten für das Unternehmen ist („charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer’s data“).

Damit wird klar, dass die Festlegung des Datenwertes in Bezug auf die Angemessenheit der Preis- oder Konditionendifferenzierung aus der Perspektive des Unternehmens erfolgt. Dies ist auch sinnvoll, da das Unternehmen sein Businessmodell danach ausrichten muss, welchen Wert die Daten für die eigene Geschäftstätigkeit haben. Dass der subjektive/individuelle Wert für die Konsumenten davon erheblich „nach oben“ oder „nach unten“ abweichen kann, ist den heterogenen Präferenzen von Konsumenten hinsichtlich ihrer Privatsphäre inhärent.¹² Das ist aber solange unproblematisch, wie die Konsumenten eine Entscheidungsfreiheit darüber haben, ob sie eine Kommerzialisierung ihrer Daten wünschen oder nicht. Sie müssen dann jedoch im Falle einer Ablehnung eine Differenzierung der Leistung des Unternehmens (Servicequalität, Serviceumfang etc.), des Preises oder sonstiger Elemente des Austauschverhältnisses von Leistung und Gegenleistung hinnehmen. Zugleich signalisiert die Formulierung des Tests, dass es einen Spielraum für die Unternehmen geben soll. So muss keineswegs der exakte Wert der Daten berechnet werden. Stattdessen genügt eine hinreichende Plausibilisierung der Berechnung des Wertes.

Parallel dazu erlaubt § 1798.125(b)(1) finanzielle Anreize („financial incentives“) für die Bereitstellung von Konsumenteninformationen, wiederum unter der Prämisse, dass dabei der „reasonably-related“-Test erfüllt wird. Ergänzend sei darauf hingewiesen, dass diese Regeln auch für die in den USA sehr verbreiteten Treueprogramme gelten, § 1798.125(b)(3).

1.3 Konkretisierung durch die CPPA

Die CPPA kann als unabhängige Behörde die datenschutzrechtlichen Vorgaben durch eigene Regeln, sog. Regulations, konkretisieren. Die entsprechende Kompetenz wurde mit Wirkung zum 21. April 2022 vom Generalstaatsanwalt auf die CPPA übertragen, § 1798.185(d). Der Erlass derartiger, für die Normadressaten bindender Verordnungen ist durch das kalifornische Verwaltungsverfahrenrecht (California Administrative Procedure Act, APA) streng geregelt. Dabei müssen unabhängige Behörden – anders als der Generalstaatsanwalt – zusätzlich eine besondere Transparenz bei den Sitzungen des Board gemäß dem Bagley-Keene-Open-Meeting-Act¹³ beachten. In diesem aufwändigen Verfahren hat sich die Behörde umfassende CCPA-Regulations gegeben, die am 29. März 2023 in Kraft getreten sind.¹⁴ Vorliegend von besonderer Bedeutung sind § 7080 CCPA-Regulations als Konkretisierung verbotener Diskriminierungspraktiken (1.3.1) und § 7081

CCPA-Regulations, der zulässige Methoden für die Berechnung des Werts der Daten nennt (1.3.2).

1.3.1 § 7080 CCPA-Regulations zum Diskriminierungsverbot

Ausgehend von einer Wiederholung des Wortlauts des § 1798.125 wird deutlich, dass es nicht um eine exakte Berechnung der Angemessenheit des Wertes der Daten geht, sondern um eine faire Schätzung (§ 7080(b) CCPA-Regulations: „good-faith estimate“). Sodann werden vier erläuternde Beispiele für unterschiedliche Fallkonstellationen genannt. Im ersten Fall eines „Freemium“-Musikstreamingdienstes muss für das im Beispiel mit 5 \$ pro Monat bepreiste Premiumangebot dargelegt werden, dass diese Zahlung in einem vernünftigen Verhältnis steht zum Wert der im zahlungsfreien Angebot verarbeiteten Konsumentendaten. Dasselbe gilt im dritten Beispiel, wenn in einem Treueprogramm Coupons oder sonstige Vorteile gewährt werden und im Gegenzug die Telefonnummer des Konsumenten verlangt wird. Dann muss der Wert dieses spezifischen Datums im Verhältnis zu den dafür gewährten Vorteilen stehen.

Im vierten Beispiel geht es um einen Online-Buchhändler, der Coupons für das Verarbeiten der Daten des Online-Nutzungsverhaltens des Konsumenten auf seiner Homepage einschließlich der Kaufhistorie und der E-Mail-Adresse gewährt. Auch diese Vorteile müssen wiederum angemessen sein in Relation zum Wert der entsprechenden Daten. Nach Auffassung der CPPA darf dabei allerdings nicht die E-Mail-Adresse erfasst werden, da diese für das Treueprogramm nicht erforderlich sei. Warum das der Fall sein soll, bleibt angesichts der Knappheit der Ausführungen allerdings unklar.

Etwas anders gelagert ist das zweite Beispiel eines Treueprogramms mit Coupons (im Beispiel im Wert von 5 \$) bei Erreichen bestimmter Umsatzsummen (im Beispiel 100 \$). Wenn der Konsument hier die Löschung seiner Daten verlangt, kann er im Gegenzug – logischerweise, möchte man ergänzen – nicht mehr am Treueprogramm teilnehmen, da dann ja seine Ausgabesummen als Grundlage für den Erhalt der Coupons dem Unternehmen nicht mehr bekannt sind. Hier ist also – zutreffenderweise – gar keine Berechnung des Wertes irgendwelcher Daten erforderlich, da der Coupon ja nicht für die Bereitstellung von Daten, sondern für bestimmte Umsätze gewährt wird und die diesbezügliche Datenerfassung sachlogisch notwendig ist, um das umsatzbezogene Treue- bzw. letztlich Rabattprogramm durchführen zu können.

Insgesamt haben diese Erläuterungsbeispiele nur einen sehr begrenzten Nutzen und tragen nur wenig zur Klärung bei. Im Ansatz machen sie aber immerhin das Spektrum deutlich, innerhalb dessen sich entsprechende Kommerzialisierungsmodelle finden lassen und wann solche nicht vorliegen (zweites Beispiel).

1.3.2 § 7081 CCPA-Regulations zu den Berechnungsmethoden

Weitere Guidance soll sodann § 7081 CCPA-Regulations zu den Methoden der Berechnung des Wertes der Daten liefern. Nach § 7081(a) CCPA-Regulations kann jedes Unternehmen eine oder mehrere dieser Methoden nutzen und dies auch dokumentieren, wobei die Aufzählung neben sieben spezifischen Ansätzen eine Auffangklausel vorsieht („Any other practical and reasonably re-

¹² Dadurch, dass der CCPA nach § 1798.140(v)(1) auch Haushaltsinformationen erfasst, weist er explizit auf eine sodann noch komplexere Frage hin, da es für Unternehmen erst recht nicht ersichtlich wäre, welchen Wert ein Haushaltsdatensatz für die gegebenenfalls mit vollkommen heterogenen Privatheitspräferenzen ausgestatteten Haushaltsmitglieder hat. Siehe grundlegend zu den Faktoren und Privatheitspräferenzen als Determinanten bei der Frage der Bereitstellung von Daten *King, Privacy, Disclosure, and Social Exchange Theory*, 2018.

¹³ Art. 9 11120 Cal. GOV; *Leblanc*, Information Today, Vol. 40 Issue 7, S. 20 (21).

¹⁴ Die CCPA-Regulations finden sich hier https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf (zul. abgerufen am 25.9.2023).

liable method of calculation used in good faith.“). Diese Auffangklausel ist auch insofern aufschlussreich, als sie die Notwendigkeit einer Praktikabilität entsprechender Bewertungsmethoden ebenso anerkennt wie den Grundsatz von „Treu und Glauben“ („good faith“) bzw. Fairness als Leitschnur für die Akzeptanz der Bewertungsmethode ausweist.

Die sieben spezifischen Methoden eröffnen den Unternehmen unterschiedliche Ansatzpunkte für die Bewertung. So können sie einerseits konkreter auf einzelne Nutzer abstellen, aber mit der dritten Methode auch den aggregierten Wert sämtlicher erfasster Daten errechnen und durch die Anzahl der Konsumenten teilen. Damit wird ein großer Spielraum für eine Pauschalierung eröffnet. Dies ist aus Praktikabilitätsgründen begrüßenswert, da kaum für alle Businessmodelle eine personenscharfe und teils gegebenenfalls nicht einmal gruppenbezogene Wertberechnung möglich sein dürfte. Außerdem dürfte das schon aus Gründen der Datensparsamkeit nicht sinnvoll sein, da zur Berechnung ansonsten eine Vielzahl zusätzlicher personenbezogener Daten verarbeitet werden müsste. Es ist auch nachvollziehbar, dass die Unternehmen wählen können, ob sie den marginalen Wert (erste Methode) des jeweiligen Konsumenten heranziehen wollen oder den Durchschnittswert (zweite Methode). Diese Werte können durchaus divergieren, da der Grenzwert des „letzten“ Konsumenten für das Unternehmen höher oder niedriger sein kann als der Durchschnittswert.

Die Methoden vier, fünf, sechs und sieben verweisen sodann letztlich auf Teilaspekte einer betriebswirtschaftlichen Kalkulation bei der Einführung von finanziellen Anreizen: Diese lohnen sich für ein Unternehmen letztlich dann, wenn zumindest in einer langfristigen Betrachtung die Einnahmen mit den generierten Daten (vierte Methode) abzüglich der Kosten für die Verarbeitung der Daten (fünfte Methode) und für die Anreize (sechste Methode) einen hinreichenden Gewinn belassen (siebte Methode). Anders formuliert wird ein Unternehmen die finanziellen Anreize so setzen, dass diese mit Blick auf die damit erzielbaren Einnahmen abzüglich der Kosten eine gewünschte Rendite generieren. Setzt das Unternehmen die Anreize zu hoch an, wird die Rendite geschmälert oder es können gar Verluste entstehen. Im umgekehrten Fall einer zu niedrigen Beanreizung werden gegebenenfalls nicht hinreichend viele Daten generiert, es drohen Einnahmeverluste und es besteht die Gefahr, dass nicht die gewünschten Gewinne erzielt werden. Dass nun jeder einzelne Faktor dieser betriebswirtschaftlichen Kalkulation als Orientierungspunkt herangezogen werden kann, unterstreicht die Flexibilität für das Unternehmen. So wird ein Start-up etwa zunächst auf Gewinne verzichten bzw. regelmäßig sogar Verluste in Kauf nehmen und daher höhere finanzielle Anreize gewähren in der Hoffnung, zu einem späteren Zeitpunkt der Skalierung diese durch erhöhte Gewinne zu kompensieren. Daher kann in einer reiferen Marktphase eine sehr hohe Rendite angestrebt werden. Damit dies nicht in die Beliebigkeit der Festsetzung der finanziellen Anreize führt, was insbesondere beim Abstellen auf die Kosten für die finanziellen Anreize offensichtlich wird¹⁵, müssen diese Berechnungsmethoden plausibilisiert werden.

Auch hier ist der Kritik zuzustimmen, dass dieser Konkretisierungstext nur recht kryptisch komplexe Berechnungsproble-

¹⁵ So könnte dies sonst den falschen Eindruck einer Zirkularität erwecken, frei nach dem in die Kontrolllosigkeit führenden Motto: Die finanziellen Anreize können orientiert an den Kosten der finanziellen Anreize festgesetzt werden.

me in der Praxis durch äußerst knapp beschriebene Methoden einzufangen versucht.¹⁶ Die Praktikabilität der aufgezeigten Methoden genauso wie mögliche weitere Berechnungsansätze müssen sich jetzt erst in der Anwendung der Regeln zeigen. Jedenfalls wird damit eine erste Indikation der vielfältigen Ansätze gegeben. Überzeugend ist auch, dass dieses Methodenspektrum den Unternehmen eine hinreichende Flexibilität eröffnet. Bei aller Kritik an der gewiss missbrauchsgefährdeten Offenheit dieses Ansatzes können fehlerhafte und unangemessene Methoden im Sinne der Konsumenten jedoch unterbunden und damit auf der Zeitschiene das Spektrum konkretisiert, ergänzt, nachgeschärft, aber auch wieder verengt werden.

1.4 Vergleichbare Entwicklungen in anderen Bundesstaaten der USA

Kalifornien ist inzwischen nicht mehr der einzige Bundesstaat in den USA mit einem umfassenden Datenschutzregime. Weitere Bundesstaaten sind dem Vorbild Kaliforniens gefolgt und haben ihre eigenen Datenschutzgesetze erlassen.¹⁷ Die meisten enthalten eine Möglichkeit zur Anpassung des Preises oder des Angebotsinhalts, wenn der Konsument von seinem Opt-out-Recht Gebrauch macht oder das Angebot mit der freiwilligen Teilnahme an Treue- und Bonusprogrammen in Zusammenhang steht. Allerdings fehlt bei den übrigen Datenschutzgesetzen regelmäßig das vorliegend umfassend analysierte Bewertungselement, wie es dem „reasonably-related“-Test innewohnt.¹⁸ Der Gesetzesentwurf für einen Consumer Personal Information Privacy Act in Alaska enthält hingegen eine mit § 1798.125 weitgehend identische Regelung.¹⁹ Ein Bewertungselement hat auch Florida eingefügt.²⁰ Insofern wird auch hier eine künftige Anwendungspraxis für den europäischen Diskurs fruchtbar gemacht werden können.

2 Berechtigte Kritik an der Regelung?

In der Literatur zur kalifornischen Regelung finden sich eine Reihe ablehnender Stimmen gegenüber diesem Ansatz. Teilweise wird der Ansatz ganz grundsätzlich in Frage gestellt (2.1), teilweise wird die Umsetzung kritisiert (2.2). Interessant ist dabei, dass die Ablehnung sowohl damit begründet wird, dass der Ansatz keinen angemessenen Schutz der Privatsphäre der Konsumenten gewährleiste,²¹ als auch umgekehrt damit, dass er für die Unternehmen schädlich sei, deren Businessmodelle – ebenfalls zum Nachteil der Konsumenten – unangemessen beeinträchtigt würden.²²

¹⁶ Kritisch etwa *Rose*, *Brook. J. Corp. Fin. & Com. L.* 15 (2021), S. 521 (534 ff.).

¹⁷ So Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Montana, Oregon, Tennessee, Texas, Utah und Virginia; vgl. zu den Entwicklungen in anderen Bundesstaaten bezogen auf § 1798.125 *Donahue*, *Loyola of Los Angeles Law Review* 56 (2023), S. 411 (456 f.).

¹⁸ Vgl. Colorado S.B. 21-190 (2021), 6-1-1308(1)(d); Connecticut S.B. 6 (2022), Sec. 6(b); Delaware H.B. 154 (2023), § 12D-106(b); Indiana SEA 5 (2023), Chapter 4 Sec. 1(4); Iowa SF 262 (2023), Sec. 4 3.; Montana S.B. 384 (2023), Sec. 7(3); Oregon S.B. 619 (2023), Sec. 5(3)(b); Tennessee S.B. 73 (2023), 47-18-3204(a)(5); Texas H.B. 4 (2023), Sec. 541.101(c); Utah S.B. 227 (2022), 13-61-302(4)(b); Virginia Consumer Data Protection Act, § 59.1-578, 4.

¹⁹ Alaska H.B. 159 (2022), Sec. 45.48.870(b).

²⁰ Florida S.B. 262 (2023), 501.71(2)(c).

²¹ Ausführlich *Donahue*, *Loyola of Los Angeles Law Review* 56 (2023), S. 411 ff.

²² Exemplarisch *Goldman*, *Technology & Marketing Law Blog* (29.6.2020), <https://blog.ericgoldman.org/>.

2.1 Fundamentalkritik

Ein Teil der Fundamentalkritik geht davon aus, dass ein Modell „Daten gegen Leistung“ in Konflikt gerät mit dem – in der kalifornischen Verfassung explizit normierten – Grundrecht auf Schutz der Privatsphäre (2.1.1). Noch fundamentaler wird die Kommerzialisierung eigener Daten prinzipiell abgelehnt (2.1.2). Schließlich wird darauf verwiesen, dass eine Berechnung eines fairen Austauschverhältnisses von Daten gegen Leistung nicht möglich sei (2.1.3).

2.1.1 Grundrechtliche Bedenken

Anders als in der US-amerikanischen Verfassung enthält Article I Section 1 der kalifornischen Verfassung explizit das Recht auf Privatsphäre („privacy“) als eines der verschiedenen unveräußerlichen Grundrechte („inalienable rights“)²³. Das schließt aber nicht aus, dass eine Abwägung mit gegenläufigen Interessen möglich wäre, wie die Rechtsprechung zu der Regelung erkennen lässt, die zunehmend sogar das Überschreiten einer gewissen Schwelle verlangt, um überhaupt einen Eingriff anzunehmen.²⁴ Warum die Kommerzialisierung der eigenen Daten dieses Recht gefährden sollte²⁵, wenn es auf der Grundlage einer freien und informierten Entscheidung erfolgt, wird bei der Kritik im Übrigen nicht hinreichend klar. Die Kritik wäre gerechtfertigt, wenn eine derartige Entscheidung per se nicht möglich wäre.²⁶ Unverständlich bleibt dabei, warum im Falle von Freiheits- und Informationsdefiziten in freiheitlicher Hinsicht nicht die Kommerzialisierungsbedingungen für die Konsumenten verbessert werden sollten, anstatt die Kommerzialisierungsmöglichkeit pauschal abzulehnen. Bei vielen anderen Vertragsverhältnissen bestehen ja gleichermaßen Freiheits- und Informationsdefizite, die Auslöser entsprechender Verbraucherschutzrechte sind, nicht aber die Austauschverhältnisse per se ausschließen, so etwa bei Kauf- und Verkaufsentscheidungen als Bestandteil der Eigentumsfreiheit der Konsumenten.

Bedenken hinsichtlich der Gewährleistung der Gleichheit²⁷ sind zwar insoweit zutreffend, als wohlhabendere Personen leichter auf die Kommerzialisierung von Daten verzichten können als ärmere Personen. Das ist aber keine Besonderheit der Ausübung des Grundrechts auf Privatsphäre, da die Ausübung sämtlicher Freiheitsrechte der kalifornischen Verfassung (wie überall) stark durch die ökonomischen Bedingungen geprägt ist – besonders augenscheinlich die Eigentumsfreiheit, aber beispielsweise auch die Sicherheit. Alle diese Rechte sind nach der Konzeption der kalifornischen Verfassung gleichermaßen unveräußerlich. Dies be-

archives/2020/06/a-review-of-the-final-ccpa-regulations-from-the-ca-attorney-general.htm (zul. abgerufen am 25.9.2023). So induzieren entsprechende Regeln unstrittig Transaktionskosten bei einer entsprechenden Compliance, die umso höher sind, je unklarer das Regelwerk ist.

²³ Siehe zum Aspekt der Unveräußerlichkeit im Zusammenhang mit der Schaffung von Marktplätzen für Daten früh bereits *Schwartz*, Harvard Law Review 117 (2004), S. 2055 (2074 ff. und 2095 ff.).

²⁴ Siehe zu der Entwicklung im Überblick *Grodin/Shanske/Salerno*, The California Constitution, 2. Aufl. 2017, Article 1, S. 53 m.w.Nachw.

²⁵ Dies aber andeutend *Donahue*, Loyola of Los Angeles Law Review 56 (2023), S. 411 (417).

²⁶ Zu den Herausforderungen diesseits und jenseits des Atlantiks dazu zuletzt aufschlussreich mit einem eigenen Ansatz, der durchaus Berührungspunkte mit dem hier verfolgten Fairnessansatz hat, *Solove*, Murky Consent. 104 Boston University Law Review (2024 im Erscheinen), II.

²⁷ *Donahue*, Loyola of Los Angeles Law Review 56 (2023), S. 411 (448 ff.).

zieht sich aber auf die prinzipielle Nutzungsmöglichkeit und nicht auf den Verzicht in einer konkreten Situation als Ausdruck der Nutzungsfreiheit. Das wäre nur anders, wenn die Privatsphäre pauschal als derart menschenwürdekernebezogen anzusehen wäre, dass sie in verfassungsrechtlicher Hinsicht nicht kommerzialisiert werden dürfte. Ein solches Kommerzialisierungsverbot liegt etwa dem Verbot des Organhandels zugrunde. Insoweit besteht jedoch keine Vergleichbarkeit – jedenfalls nicht für das Gros der Datenverarbeitungsvorgänge.

2.1.2 Ablehnung der Kommerzialisierung eigener Daten

Letztlich steht hinter den grundrechtlichen Argumenten die rechtspolitische Ablehnung einer Kommerzialisierung eigener Daten. Neben dem Gleichheitsargument wird in rechtspolitischer Hinsicht die mangelnde Entscheidungsfähigkeit der Konsumenten angeführt, die, so die Kritik teils explizit, paternalistische Strukturen verlange²⁸. Der Konsument soll gleichsam nicht (nur) vor dem Unternehmen geschützt werden, sondern (auch) vor sich selbst. Das ist jedoch nur insoweit überzeugend, wie nachgewiesen werden kann, dass Konsumenten letztlich Entscheidungen treffen, die sie eigentlich nicht treffen wollen. Auch hier stellt sich wiederum die Frage, warum das zu einem Ausschluss von Handlungsmöglichkeiten für Konsumenten führen soll (auch in der Variante einer Kommerzialisierung ihrer Daten) und nicht zu einer besseren Aufklärung, zu mehr Transparenz, zur Einräumung von Handlungsalternativen bis hin zu einer Disziplinierung der Unternehmen im Sinne einer entsprechenden Fairness. Letztlich teilt diese Kritik hinsichtlich der Möglichkeit einer eigenbestimmten Privatsphäre den Skeptizismus mancher Vertreter von Big-Data-Unternehmen.²⁹ Den Verfechtern eines paternalistischen Privatsphäreschutzes zufolge soll dies aber nicht zu einer Freigabe der Datenverarbeitung führen, sondern zu deren Verbot. Beides schafft jedenfalls keine Stärkung der Verbrauchersouveränität. Viel sinnvoller ist es stattdessen, an der Ertüchtigung der Verbrauchersouveränität durch die Verbesserung der Rahmenbedingungen in puncto Informiertheit, Optionenvielfalt, Standardisierung von Entscheidungsprozessen bis hin zum Einsatz von Intermediären³⁰ zu arbeiten.

2.1.3 Unmöglichkeit der Berechnung

Dasselbe gilt für die pauschale Skepsis gegenüber der Möglichkeit, angemessene Berechnungsmethoden zu entwickeln.³¹ Wäre eine exakte Berechnung des Wertes aus der Perspektive des Konsumenten erforderlich, träfe diese Skepsis sicherlich zu. Aber, wie dargelegt (1.2 und 1.3), geht es ja lediglich um eine Plausibilisierung der Angemessenheit aus der Perspektive des Wertes der Daten für das Unternehmen. Im Übrigen unterschätzt die skeptische Position letztlich das Entwicklungspotenzial entsprechender Bewertungsmodelle über die Zeit hinweg und die Ertüchtigungsmöglichkeiten für die Konsumenten: Durch eine Verfeine-

²⁸ *Donahue*, Loyola of Los Angeles Law Review 56 (2023), S. 411 (457).

²⁹ Berühmt insoweit die Äußerung des damaligen CEO von Sun Microsystems Scott McNealy aus dem Jahr 1999: „There is zero privacy anyway, get over it.“, siehe <https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> (zul. abgerufen am 25.9.2023).

³⁰ Zu den damit verbundenen Herausforderungen etwa *Kühling*, ZfDR 2021, 1 ff.; *ders.*, DuD 2021, 783 ff. (leicht aktualisierte und gekürzte Fassung).

³¹ *Donahue*, Loyola of Los Angeles Law Review 56 (2023), S. 411 (431 ff.).

rung der Methodik und die Etablierung entsprechender Handlungsalternativen wird dem Verbraucher der Wert seiner Daten viel bewusster und klarer. So wie beim Erwachsenwerden der Wert des Geldes erst erlernt werden muss (etwa bezogen auf den Arbeitseinsatz, der zu dessen Generierung erforderlich ist, oder die Opportunitätskosten eines Kaufes eines Produktes zu einem bestimmten Zeitpunkt im Vergleich zu späteren Möglichkeiten des Geldeinsatzes), wäre hier das Leitbild souveräner Konsumenten, dass sie den Wert ihrer Daten erlernen. Dass sodann Präferenzen divergieren können, ist ebenso unproblematisch wie der unterschiedliche subjektive Wert von Gütern (etwa die Mitgliedschaft in einem Fitnessclub). Aufgabe der Datenschutzbehörden und der Wissenschaft ist es daher, die Berechnungsmethodik zu verfeinern und zugleich die Konsumentensouveränität bei Entscheidungsprozessen zu erhöhen.

2.2 Kritik an der Umsetzung

An der Umsetzung wird sodann die Unklarheit der konkreten Regelungen im kalifornischen Recht kritisiert³² (2.2.1) – regelmäßig in Ergänzung einer Fundamentalkritik am Ansatz. Allerdings gibt es auch Analysen, die den Ansatz prinzipiell gutheißen, aber die Umsetzung für nicht weit gehend genug halten zum Schutz der Privatsphäre. Dabei wird insbesondere für einen Opt-in-Ansatz plädiert (2.2.2).

2.2.1 Unklarheit der Regelung

Die Ausführungen unter 1.3 haben gezeigt, dass unter Rückgriff auf die weiteren Konkretisierungen durch die §§ 7080, 7081 CCPA-Regulations zumindest ein erster Aufschlagpunkt für die Unternehmen geschaffen wurde. Sie verfügen über einen gewissen methodischen Spielraum, müssen ihre Berechnungsmodelle aber dokumentieren und auch plausibilisieren können. Es kommt im Übrigen auf den Wert der Daten für ihr Unternehmen an. Sie können hinsichtlich der verschiedenen Konsumenten und Konsumentengruppen recht frei differenzieren oder auf eine Differenzierung verzichten, wenn es dafür plausible Gründe gibt. Diese können gerade auch in der Praktikabilität – und sinnvollerweise wohl auch in der Datensparsamkeit – begründet sein. Das sind jedenfalls deutlich konkretere Ausgestaltungshinweise als sie bislang unter der DSGVO entwickelt wurden (dazu sogleich 3.).

2.2.2 Opt in statt Opt out

Aus der Perspektive einer Zustimmung zum Grundansatz wird teilweise kritisiert, dass die Regelung im kalifornischen Recht zu kurz greift. So gehe sie – sofern es sich nicht um besonders sensible Daten handele – immer noch vom Opt-out-Ansatz aus³³. Ein Opt-in-Ansatz würde einen stärkeren Schutz der Privatsphäre leisten. Dem ist grundsätzlich zuzustimmen. Dies hat bei der DSGVO dazu geführt, dass im Rahmen der Einwilligung ein Opt-in-Ansatz greift.³⁴ Die Einführung der Verpflichtung für Unternehmen zur Bereitstellung eines permanenten Opt-out-Signals durch den CCPA relativiert die Schärfe des Unterschieds jedoch

erheblich. Insgesamt ist von der Etablierung eines fairen Rahmens für eine Kommerzialisierung der Daten zu erhoffen, dass die gesteigerte Konsumentensouveränität und die Eröffnung von Handlungsoptionen sowie die Schaffung von echten, bewussten und informierten sowie praktisch einfach handhabbaren Wahlmöglichkeiten den Unterschied weiter relativieren. Unabhängig davon ist das europäische Modell insoweit im Ausgangspunkt tatsächlich datenschutzfreundlicher, das kalifornische dagegen unternehmensfreundlicher.

3 Konvergenz von DSGVO und CCPA

Damit schafft das kalifornische Recht einen an der Angemessenheit orientierten Rahmen für das Geschäftsmodell eines Austauschs von Daten gegen Leistungen. Dies entspricht der in der Literatur vielfältig vertretenen Auslegung des Einwilligungstatbestands nach Art. 7 DSGVO.³⁵ Den Ansatz hat jüngst auch der EuGH im Meta-Urteil bestätigt,³⁶ als er an die Rechtmäßigkeit der Einwilligung gegenüber einem quasimonopolistischen Anbieter wie Meta („klares Ungleichgewicht“ im Sinne des EG 43 der DSGVO, siehe Ziff. 149 der Entscheidung) zu Recht strenge Anforderungen gestellt hat, aber die Zahlung mit Daten im Rahmen einer einwilligungsbasierten Verarbeitung für den Fall als zulässig ansieht, dass Meta „eine gleichwertige Alternative“ anbietet. Dafür dürfe Meta dann auch „ein angemessenes Entgelt“ verlangen (Ziff. 150).³⁷ Näher konkretisiert der EuGH dies nicht.

Ein entscheidender Unterschied besteht dabei insoweit, dass die kalifornische Regelung keineswegs auf marktdominante Unternehmen beschränkt ist, sondern sämtliche Unternehmen erfasst. Der Ansatz reicht damit – jedenfalls nach dem bisherigen Stand der Interpretation der DSGVO – deutlicher weiter als die europäische Regelung. Dies kann rechtspolitisch durchaus hinterfragt werden. Für Konsumenten besteht gegenüber nicht marktdominanten Unternehmen jedenfalls eine größere Reaktionsflexibilität, da einfacher auf andere Anbieter mit alternativen Angeboten in puncto Datenschutz zurückgegriffen werden kann. Die Datensouveränität kann also mit Blick auf verschiedene Anbieter verwirklicht werden und muss nicht durch verschiedene Angebote eines (marktdominanten) Anbieters gewährleistet werden.

Die Ausgangspunkte sind im Übrigen auch insoweit signifikant verschieden, als das Modell der DSGVO vom Opt in und nicht vom Opt out ausgeht und nicht eine Situation behandelt, in der ein Unternehmen von sich aus eine Preisdifferenzierung je nach Umfang der Verarbeitung von Daten des Vertragspartners anbietet und dies rechtfertigen möchte. Ausgangspunkt ist vielmehr, dass ein (marktdominantes) Unternehmen letztlich dazu gezwungen wird, diese zahlungsbasierte Option überhaupt erst einzuführen. Dieser Unterschied relativiert sich jedoch dadurch, dass das kalifornische Recht ja ein Opt-out-Recht der Datenverarbeitung einführt, das im Falle einer faktisch häufigen Nutzung zum Angebot von Preis- und Konditionendifferenzierungen zwingt. Jedenfalls wird im Ergebnis bei beiden Ansätzen die Souveränität der natürlichen Personen dadurch gestärkt, dass sie über entsprechende Optionen verfügen, eine bewusste Wahl treffen können und die Alternativen in einem angemessenen Verhält-

32 Kritisch etwa Rose, Brook. J. Corp. Fin. & Com. L. 15 (2021), S. 521 (533 ff.).

33 Den Opt-out-Ansatz kritisierend Harris, Loyola of Los Angeles Law Review 54 (2020), S. 197 (230 ff.).

34 Buchner/Kühling in Kühling/Buchner, DS-GVO/BDSG, 4. Aufl. 2024 (im Erscheinen), Art. 7, Rn. 12, 56 ff., 58.

35 Buchner/Kühling in Kühling/Buchner, DS-GVO/BDSG, 4. Aufl. 2024 (im Erscheinen), Art. 7, Rn. 52 ff., 53c, 54.

36 EuGH, Urt. v. 4.7.2023, C-252/21 – Meta, ECLI:EU:C:2023:537, DuD 2023, 579.

37 Zustimmend Kühling/Buchner, DuD 2023, 519 (520).

nis stehen müssen. Durch die normative und objektive Bewertung der Optionen unter einem Fairnessmaßstab wird ein Schutz der Konsumenten bzw. Betroffenen gewährleistet, ohne paternalistisch als datenschutzfeindlich angesehene Möglichkeiten per se auszuschließen. Damit wird zugleich für die Unternehmen ein hinreichender Spielraum gewahrt, der im Ergebnis für die Konsumenten überhaupt erst eine entsprechende Angebotsvielfalt ermöglicht. Die Konkretisierungstiefe im kalifornischen Recht ist dabei schon weiter vorangeschritten und eine künftige Anwendungspraxis kann zusätzliche Klarheit schaffen. Dass es sehr schnell zu einer hohen Compliance mit diesem Ansatz kommt, ist allerdings angesichts der im Vergleich zur DSGVO deutlich geringeren Sanktionsmöglichkeiten im CCPA (siehe § 1798.155³⁸) unklar und dürfte stark von den Durchsetzungsprioritäten der CPPA oder entsprechenden Konsumentenklagen abhängen.

4 Fazit

Ausgangspunkt für die kalifornische Regelung war – anders als im Unionsrecht – eine weit verbreitete und wenig reglementierte Bereitstellung von Daten gegen Leistung. Diese fußte auf dem sehr liberalen US-amerikanischen Einwilligungskonzept, das im Wege eines „notice and choice“ im Wesentlichen einen Hinweis auf die Datenverarbeitungsregeln vor Bereitstellung der Dienste als Legitimation genügen lässt.³⁹ Die kalifornische Regelung des Modells „Daten gegen Leistung“ ist vor diesem Hintergrund als normative Umhegung und Eingrenzung zu verstehen und jedenfalls grundsätzlich zu begrüßen. Der Ausgangspunkt im Unionsrecht ist in gewisser Weise umgekehrt, da hier strenge Anforderungen an die Akzeptanz des Modells gestellt werden und es teilweise – zu Unrecht⁴⁰ – als unionsrechtswidrig angesehen

³⁸ Dazu im Überblick *Illmann/Temple*, *The Business Lawyer* 75 (2020), S. 1637 (1644 f.). Besonders fraglich mit Blick auf die unmittelbare Compliance ist die Regelung in § 1798.199.50, die einen Verstoß nur dann annimmt, wenn die Unternehmen eine Anpassung ihres Verhaltens nicht binnen 30 Tagen nach einem Hinweis durchführen.

³⁹ Zu diesem unterschiedlichen Ausgangspunkt im Vergleich zum Ansatz der DSGVO umfassend und informativ *Solove*, *Murky Consent*. 104 *Boston University Law Review* (2024 im Erscheinen), II.

⁴⁰ Zur Sonderfrage, inwiefern der DMA in Art. 5 Abs. 2 ein solches Modell für Gatekeeper einschränkt, instruktiv in diesem Heft *Schmid/Späth und dies.*, *NZKart* 2022, 568.

hen wird. Hier geht es darum, im Sinne einer Datensouveränität ein sinnvoll ausgestaltetes Modell rechtlich abzusichern. Die kalifornische Regelung kann angesichts der bereits erfolgten stärkeren Konkretisierung für die Fortentwicklung des durchaus vergleichbaren Ansatzes in der DSGVO – wie zuletzt vom EuGH im Meta-Urteil bestätigt – wegweisend sein. Eine derartig – trotz aller verbleibender Unterschiede – in Teilen konvergente Entwicklung wäre sicherlich auch für die betroffenen Unternehmen von Vorteil, die so einen einheitlichen Standard entwickeln können. Diese Konvergenz kann zudem ein Schritt sein, die an sich so separaten Datenschutzansätze diesseits und jenseits des Atlantiks wieder näher zusammenzubringen.

Auch in der Sache ist das Modell jedenfalls im Ansatz zu begrüßen, stärkt es doch die Souveränität der Grundrechtsträger. Um diese tatsächlich zu schützen, bedarf es allerdings einer weiteren Fundierung der Bewertungsmethoden in Wissenschaft und Entscheidungspraxis, ebenso wie die „umrahmenden“ Anforderungen an die Transparenz und Information weiter geschärft werden müssen. Hier könnte es ein Vorzug des Ansatzes der DSGVO sein, dass diese mit Art. 5 lit. a, aber auch im Übrigen umfassend auf eine Fairness in der Datenverarbeitung angelegt ist, sowohl was die materiell-rechtliche als auch was die formelle Steuerung der entsprechenden Prozesse anbelangt. Dies muss jedoch mit Blick auf das Konzept „Daten gegen Leistung“ erst noch ausbuchstabiert werden.

Open Access

Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 (CC BY) International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/ die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Funding

Open Access funding enabled and organized by Projekt DEAL.

Neues aus der Reihe „Die blaue Stunde der Informatik“



G. Müller
Protektion 4.0: Das Digitalisierungsdilemma
Reihe: Die blaue Stunde der Informatik

2020, XI, 241 S. 34 Abb. Geb.

€ (D) 49,99 | € (A) 51,39 | *CHF 55.50 | ISBN 978-3-662-56261-1

€ 39,99 | *CHF 44.00 | ISBN 978-3-662-56262-8 (eBook)

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D): gebundener Ladenpreis in Deutschland, € (A): in Österreich.

*: unverbindliche Preisempfehlung. Alle Preise inkl. MwSt.

Jetzt bestellen auf springer.com/informatik oder in der Buchhandlung

Part of **SPRINGER NATURE**