LEGAL REVOLUTIONary
Rechtsmagazin der digitalen Wirtschaft

50 Jahre Datenschutz

Die überfällige Reform durch eine neu definierte Datensouveränität

Dr. Ulrich Seidel | Rechtsanwalt

24. August 2020

LR 2020, Seiten 229 bis 234 (insgesamt 6 Seiten)

Die vielzitierte und vielbeschriebene Datensouveränität ist ein schillernder Diskursbegriff und entbehrt - anders als der Datenschutz (vgl. Rn. 16 unten, Anmerkung 1) - einer allgemein anerkannten Definition. Im Rahmen der fortschreitenden Digitalisierung der Gesellschaft, die nicht zuletzt durch die Corona-Krise eine deutliche Beschleunigung erhalten hat und noch erhalten wird, besteht sogar ein steigender Bedarf an der Klärung dieses Begriffes. 1

Oftmals wird Datensouveränität von Datenschützern als unbestimmter „Lobbybegriff" der Wirtschaft kritisiert oder er wird als die digitale Kompetenz und Fähigkeit des Einzelnen im Umgang mit den digitalen Medien verstanden. Darüber hinaus gibt es noch zahlreiche Einzelmeinungen. Eine Tendenz bildet sich allerdings dahingehend heraus, dass personenbezogene Daten nun als Zahlungsmittel für Leistungen im Internet gehandelt werden und somit zu einer Monetarisierung und Kommerzialisierung führen. Man darf davon ausgehen, dass der Gesetzgeber diese faktische Tendenz im Rahmen eines mit neuen Verfügungsrechten ausgestatteten Datenschuldrechts und einer schwierigen Klärung des Verhältnisses zum gegenwärtigen Datenschutzrecht wird regeln müssen. Ein allgemein anerkanntes Verständnis des Begriffes der Datensouveränität hat sich aber noch nicht etabliert. 2

Angesichts dieser Unsicherheit und des dringenden Bedarfs an einer allgemein anerkannten Definition wird deshalb die Begriffsbildung in der unter der Anmerkung 2 (Rn. 16 unten) genannten Publikation zusammenfassend erläutert und aktualisiert. 3

Im gegenwärtigen Datenschutzrecht nimmt der Einzelne die Rolle eines passiv geprägten Datensubjektes ein - verbunden mit gewissen Rechten, wie z.B. auf Auskunft, Löschung, Berichtigung etc. seiner personenbezogenen Daten. Die Entscheidung über die Verarbeitung der Daten liegt jedoch bei den Verantwortlichen als datenverarbeitenden Stellen. Das Datensouveränitätsrecht betrachtet demgegenüber personenbezogene Daten als alle von einer natürlichen Person selbst generierten und zweckbestimmt verwendeten Informationen über ihre wirtschaftlichen, sozialen, kulturellen, gesundheitlichen etc. Merkmale. Der Einzelne fungiert somit als gestaltender Akteur seiner Datenverarbeitungsprozesse statt nur als 4

passives Datensubjekt. Anders formuliert:

Datensouveränität bezeichnet den Anspruch einer natürlichen Person gegenüber einem Verantwortlichen auf voreingestellte Möglichkeiten für einen selbst gestaltbaren Umgang ihrer personenbezogenen Daten.

Im Zeitalter von Big Data und den schier unendlich vielen Verknüpfungsmöglichkeiten von personenbezogenen Daten und dem daraus resultierenden Erkenntnisgewinn über menschliches Verhalten ist davon auszugehen, dass praktisch alle personenbezogenen Daten geldwerte Daten und damit disponible Wirtschaftsgüter darstellen. *Das Datensouveränitätsrecht betrachtet personenbezogene Daten im Wesentlichen als Wertmerkmale anstatt als reine Wissensmerkmale wie im Datenschutzrecht*. Der „Verkauf" oder die Lizenzübertragung personenbezogener Daten wird als Ausdruck der umfassend verstandenen Verfügungsmacht des Einzelnen über seine personenbezogenen Daten von der Datensouveränität mit umfasst, steht aber nicht im Vordergrund. 5

Die sog. *Voreinstellungssouveränität* liegt im Datensouveränitätsrecht beim Verantwortlichen, die *Datenverwendungssouveränität* bei den Betroffenen bzw. Datengebern, also jedem Einzelnen. Die souveräne Ausübung dieser Datenverwendung dient der ökonomischen Steuerung des persönlichen, digitalen Rechtsverkehrs. Datensouveränität knüpft insoweit an den Grundsatz der Privatautonomie an. Gerade aufgrund des heutigen Stellenwertes von Daten sowie der dem Einzelnen zur Verfügung stehenden stationären und mobilen Datenverarbeitungskapazität ist es nicht länger hinnehmbar, personenbezogene Daten nur als Hilfsmittel zur Erfüllung vertraglicher Aufgaben oder etwa im Rahmen einer statisch vorformulierten Einwilligung zu betrachten und den Einzelnen – ohne echte eigene Gestaltungsmacht – lediglich gegen einen missbräuchlichen Umgang seiner Daten zu schützen. 6

Da die eigentumsrechtliche Betrachtung personenbezogener Daten (Daten sind keine Sachen) als gescheitert gilt, bedarf es spezifischer Souveränitätsrechte als Gestaltungs-, Verfügungs- und Transformationsrechte. In Betracht kommen fünf neue dem Einzelnen zustehenden Datenrechte: 7

1. Anspruch auf Zurverfügungstellung individuell wählbarer und änderbarer Sachverhaltsbausteine anstatt – wie bisher – Vorlage eines feststehenden ganzheitlichen Sachverhaltes. Solche Bausteinverträge werden zwar immer häufiger, sind aber oftmals (auch bezüglich der Datenverwendung) einseitig im Interesse der datenverarbeitenden Stellen formuliert.
2. Anspruch auf verknüpfbare Auswahlmöglichkeiten zu anderen Sachverhalten, insbesondere verknüpfbarer sektorspezifischer und -übergreifender Art. Die Gestaltung verfügbarer Verknüpfungen kann durch Inferenztechniken (Schlussfolgerungstechniken) der künstlichen Intelligenz unterstützt werden.

3. Anspruch auf quantitativ optimierbare Datenverwendungsmodelle und Nutzungsbilanzen, insbesondere im Rahmen langfristiger Rechtsverhältnisse.
4. Anspruch auf mögliche Umwandlung entgeltlicher Wertkonten, beispielsweise Umwandlung von Lebensarbeitszeitkonten in Rentenleistungen oder flexible Arbeitszeitmodelle.
5. Anspruch auf Portierung / Übertragung rechtsverbindlich geregelter oder vereinbarter Datensachverhalte auf anderweitige Rechtsverhältnisse. An der Portierbarkeit von Sachverhalten – z.B. von Zeitwertkonten – besteht ein großer Bedarf, hängt jedoch bis heute z.B. von der Mitwirkung des neuen Arbeitgebers ab. Dieses Portierungsrecht ist nicht mit der Datenportabilität der DS-GVO zu verwechseln, bei der es lediglich um die „Mitnahme" von gewissen selbst zur Verfügung gestellten Daten zu einer anderen datenverarbeitenden Stelle geht.

Bei den voreinzustellenden Sachverhaltsdaten handelt es sich nicht um personenbezogene Daten gem. Art. 4 Nr. 1 DS-GVO, sondern um *öffentlich frei zugängliche Sachdaten. Erst über die Ausübung der Verwendungssouveränität, nämlich durch die Auswahl bestimmter Möglichkeiten entstehen dem Einzelnen zuzuordnende personenbezogene Daten.* Die Schnittstelle zwischen Datenschutz und Datensouveränität führt dazu, *dass eine informierte und freiwillige Einwilligung gem. Art. 6 UAbs. 1 lit. a), 7 DS-GVO für eine zulässige Datenverarbeitung alleine nicht mehr ausreichen würde, sondern vielmehr eine souveräne Einwilligung auf Basis auswählbarer Verwendungs- und Nutzungsansprüche erforderlich ist.* Der Sinn der datenschutzrechtlichen Einwilligung in ihrer gegenwärtigen Ausgestaltung als Legitimation für eine rechtmäßige Datenverarbeitung ist ohnehin seit längerem umstritten. Sie wird nicht selten auf Basis von unverständlichen sowie unvollständigen Einwilligungserklärungen eingeholt und ist in der Praxis zu einer lästigen Pflichtübung ohne erkennbaren Nutzen für den Einzelnen denaturiert. 8

Zudem ist der heilige Gral der „Freiwilligkeit" längst eine Farce geworden. Obwohl die Einwilligung in der Praxis nach wie vor eine wichtige Legitimationsgrundlage darstellt, wird die Freiwilligkeit der Einwilligung in der DS-GVO nur erwähnt, nicht aber konkret definiert. Zudem ist das *Koppelungsverbot*, welches ebendiese nur erwähnte Freiwilligkeit gewährleisten soll, nicht als absolutes Verbot formuliert. Auch durch diese gesetzlichen Webfehler wird die Freiwilligkeit in der Praxis weitgehend ausgehöhlt und es ist genau das eingetreten, was vermieden werden sollte: Verweigert der Betroffene die Einwilligung in einem Sacherhalt, der vom Anbieter mit der gewünschten Dienstleistung gekoppelt wird, obwohl dies nicht unbedingt angebracht oder erforderlich ist, wird die gewünschte Dienstleistung schlichtweg nicht erbracht. Die Vorgabe der DS-GVO, dass verschiedene Verarbeitungsvorgänge auch verschiedene, voneinander unabhängige Einwilligungen voraussetzen müssen, ist weitgehend gescheitert. 9

Erst das Kartellrecht muss dem Datenschutz Schützenhilfe leisten, wie die jüngste Facebook-Entscheidung des BGH (Beschl. v. 23.06.2020, KVR 69/19) zeigt: Das soziale Netzwerk missbraucht seine marktbeherrschende Stellung, weil es eine umfassende Datensammlung bei seinen Nutzern vornimmt (nämlich auch dann, wenn die Nutzer Seiten außerhalb von Facebook besuchen), ohne hierfür eine gesonderte Einwilligung einzuholen. Dabei ist der BGH offenbar davon ausgegangen, dass die Wahl bei Facebook (entweder mitmachen und einmalig in verschiedene Verarbeitungsvorgänge gebündelt bzw. gekoppelt einwilligen oder draußen bleiben) nach dem „Friss oder stirb"-Prinzip erfolgt und gerade keine echte oder freie Wahl darstellt. Somit macht Facebook nichts anderes als Unternehmen, die einen Vertrag nur abschließen, wenn der Betroffene beispielsweise gleichzeitig auch einen Newsletter bestellt: Es werden unabhängige Sachverhalte zu einem feststehenden Sachverhalt gekoppelt, dem sich der Betroffene entweder insgesamt unterwirft oder eben vollständig fernbleibt. 10

Diese Webfehler werden durch die Datensouveränität beseitigt, die damit die Legitimationsgrundlage der informierten und freiwilligen Einwilligung um das Merkmal *souverän* ergänzt. Die Unterteilung eines Sachverhaltes in selbständig wählbare Bausteine liegt nicht mehr länger nur in der Macht der Verantwortlichen, also den Anbietern von Produkten / Dienstleistungen, sondern entwickelt sich zu einem Anspruch des Einzelnen gegenüber den Verantwortlichen und macht den Einzelnen damit souverän. Die mit dieser Entwicklung einhergehende Vielzahl von Einwilligungen könnte über die Schnittstelle zur Datensouveränität durch einzelne, breit gefächerte Datenvollmachten ergänzt oder sogar weitgehend ersetzt werden. Diese Datenvollmachten formulieren automatisiert eine Vielzahl von souveränen Einwilligungserklärungen auf der Basis einer durch den Einzelnen selbst ausgeübten Datenverwendung mit der Folge von rechtsverbindlichen Verträgen. 11

Die Anforderungen an die von den Verantwortlichen voreinzustellende Datensouveränität müssen einer gesetzlichen und richterlich voll überprüfbaren Inhaltskontrolle unterliegen, ähnlich der Gesetzgebung zu den allgemeinen Geschäftsbedingungen. Hierbei sind Kriterien für sektorspezifisch angemessene, aber auch substantielle Souveränitätsspielräume zu entwickeln, auch mit Verboten bei missbräuchlich voreingestellten Gestaltungsmöglichkeiten. Verantwortliche können zudem durch präferierte Voreinstellungen, wie z.B. Incentives (insbesondere Rabattierungen, Boni- oder Malifikationen), das Entscheidungsverhalten der Betroffenen bei der Inanspruchnahme wählbarer Angebote beeinflussen. 12

Die notwendigen Datensouveränitätsgesetze müssen über F&E-Projekte erarbeitet und erprobt werden, insbesondere im Bereich einer mobilen und hochflexiblen Arbeitszeitsouveränität, einer selbstgestaltbaren Tilgung von Kreditdaten, einem souveränen Umgang von Fahrzeug- und Wohnungsdaten, einer Emissionsdatensouveränität in diversen Rechtsverhältnissen, einer digitalen Gesundheitssouveränität als flankierende Maßnahme zur elektronischen Gesundheitskarte oder einer souveränen Kontrolle und Vermarktung von 13

Kundendaten.

Im Bereich der Arbeitszeitsouveränität gibt es alleine mindestens 20 konfigurierbare Sachverhaltsbausteine mit millionenfach unterschiedlich möglichen Verknüpfungen zur Erfüllung von Arbeitszeitpflichten, z.B. Gleitzeit, Teilzeit, Altersteilzeit, Mehrarbeitszeit, Minderarbeitszeit, Home Office-Zeit, Erholungsurlaub, Bildungsurlaub, Sonderurlaub, Sabbatical, Elternzeit, Kindererziehungszeit, Pflegezeit, Kurzarbeitszeit, Schichtarbeitszeit, Schlechtwetterarbeitszeit, Nachtarbeitszeit, Vorruhestandszeit. Bei der Kreditdatensouveränität sind unterschiedlichste Tilgungsrechte möglich, die über die bisher üblichen Möglichkeiten von Stundungen, Sondertilgungen, Tilgungsersatzleistungen etc. weit hinausgehen. Kunden-, Wohnungs- oder Fahrzeugdaten *haben bereits heute einen beträchtlichen Marktwert und könnten – in Ausübung der Datenverwendungssouveränität* – diversifiziert in vielschichtigen Zusammenhängen wirtschaftlich verwertet werden. Insbesondere die Corona-Krise hat einen enormen Bedarf offengelegt, komplexe und langfristig angelegte Rechtsverhältnisse selbstgestaltbar kreativ anzupassen, um existentielle Brüche rechtlicher Bindungen zu vermeiden. Dabei wäre diese technisch anspruchsvoll ausgerichtete Datensouveränität in den Rahmen der neu aufgelegten High Tech-Forschungs- und Innovationsprojekte von Bund und der EU aufzunehmen. 14

Die Datensouveränität stellt neue Anforderungen an die Gesetzgebungstechnik. Erst kürzlich ist die von Juristen seit langem vernachlässigte Legistik von der Gesellschaft für Gesetzgebung als neu einzurichtendes Unterrichtsfach wieder aufgegriffen worden. Die Datensouveränität betrachtet Gesetze als Regelungsbaukästen, in denen voreingestellte Rechtssätze selbstgestaltbar ausgewählt und unmittelbar rechtskräftig angewendet werden können. Diese Gesetzgebungstechnik führt zu einer deutlich erhöhten rechtlichen Effizienz. Im wirtschaftlichen Rechtsverkehr verringert sie den Anfechtungs- und Rechtsmittelbedarf des Einzelnen gegenüber seinen Vertragspartnern und der vollziehenden Gewalt im öffentlichen Recht und damit verbunden auch den justiziellen Prüfungsbedarf. Die klassische Gesetzgebungstechnik entwickelt sich dann zu einer gesetzgeberischen Infrastruktur mit regelungstechnischen Werkzeugen für eine digital unterstützte Einzelfallsregulierung. Im Rahmen der beschriebenen F&E-Projekte wäre dieses innovative Konzept einer digitalen Legistik anwendungsnah zu erproben. Im Bereich der Wirtschaft könnte die so definierte Datensouveränität zu einer Vielzahl innovativer datenanalytischer Geschäftsmodelle führen, was von der Politik und Wirtschaft seit langem gefordert wird. Im Ergebnis ist Datensouveränität einerseits die erweiterte Legitimationsgrundlage im Datenschutzrecht für eine informierte und freiwillige Einwilligung und andererseits eine digitale Regulierungstechnik für eine fortschreitend individualisierte und unmittelbar geltende bzw. verbindliche Rechtsanwendung. 15

Anmerkung: 16

1. Der Begriff des Datenschutzes ist nicht, wie von einigen behauptet, unbekannten Ursprungs, sondern geht in seiner nach 50 Jahren immer noch international gültigen Definition auf die wissenschaftliche Publikation von Seidel, Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, NJW 1970, 1581 ff. zurück. In diesem Beitrag wurde der Datenschutz von dem Verständnis als betriebliche Datensicherheit, das noch dem Hessischen Datenschutzgesetz vom Oktober 1970 zugrunde lag, abgetrennt und dem Persönlichkeitsrecht als Regelung personenbezogener Datenverarbeitung zugeordnet, vgl. Zielinski, Literaturschau: Rechtsinformatik, JuS 1973, 130 (131). Die Begriffsbildung setzte sich auch gegenüber den Vorschlägen eines Informationsschutzes durch, vgl. Datenschutz – Datensicherung, Beiträge zur integrierten DV in der öffentl. Verwaltung, Heft 5, Siemens, Nov. 1971; des weiteren Wikipedia (https://de.wikipedia.org/wiki/Datenschutz – Abschnitt „Begriffe und wissenschaftliche Begründungen"), FifF-Kommunikation 2/2015, S. 62 ff. mit jeweils weiteren Nachweisen und einem Abdruck der oben zitierten Publikation von 1970 (https://www.fiff.de/publikationen/fiff-kommunikation/fk-2015/fk-2015-2/fk-2015-2-content/fk-2-15-s62.pdf). Zur Begründung des Datenschutzes durch den Verfasser auch Humboldt-Uni Berlin, 50 Jahre Datenschutz in Deutschland (https://blogs.hu-berlin.de/hu_gpr/2020/02/26/50-jahre-datenschutz-in-deutschland/). Der Verfasser gilt auch als „Erfinder" des informationellen Selbstbestimmungsrechts, das er ohne den Zusatz „informationell" als Selbstbestimmungsrecht, Informationen vorzuenthalten oder mitzuteilen, bezeichnet, vgl. Pohle, Datenschutz und Technikgestaltung, Berlin 2016, S. 34 ff. (https://edoc.hu-berlin.de/handle/18452/19886).

2. Dieser Beitrag ist eine Zusammenfassung sowie ein Update der Publikation: Seidel, Grundrecht auf Datensouveränität, ZG 2014, 153 ff.