Grundwissen

Daten und ihr Schutz im Kontext von Gesellschaft, Geschichte und Recht

Fabio Stark

Fabio Stark wurde 1996 in Starnberg geboren und studiert seit 2017 Rechtswissenschaften an der LMU München mit dem Schwerpunkt Wettbewerbsrecht und Geistiges Eigentum.

Open Peer Review

Dieser Beitrag wurde lektoriert von: Hendrik Eppelmann und Isabel Lihotzky

Data is the new oil. Es soll der britische Mathematiker und Entrepreneur *Clive Humby* gewesen sein, der diese vielzitierte Analogie 2006 erstmals verwendet hat. Und tatsächlich – zumindest ökonomisch betrachtet – bestehen zwischen den zwei „Rohstoffen" einige Gemeinsamkeiten: Erstens bedarf es in beiden Fällen eines irgendwie gearteten Gewinn- und Verarbeitungsprozesses, um unmittelbaren Nutzen aus ihnen ziehen zu können. Zweitens zählen jene Unternehmen, die sich mit Gewinn und Verarbeitung der jeweiligen Ressource auseinandersetzen, zu den weltweit erfolgreichsten Unternehmen ihrer Zeit.

„Data is the new oil."

Waren es 2008 noch die Ölkonzerne *ExxonMobil*, *PetroChina*, *Gazprom* und *PetroBras*, so sind es heute die datenspezialisierten *GAFAM*-Unternehmen (*Google*, *Apple*, *Facebook*, *Amazon* und *Microsoft*), die nicht nur als die wertvollsten Marken der Welt gelten, sondern auch über erheblichen marktwirtschaftlichen und politischen Einfluss verfügen. Und schließlich stütz(t)en sich ganze Wirtschaftszyklen, wie das *Zeitalter des Schwarzen Golds* und die *Data Economy*, auf die mittelbare oder unmittelbare Kommerzialisierung von Rohöl oder Daten.

So einleuchtend der Vergleich also auf den ersten Blick auch sein mag, sollte er nicht darüber hinwegtäuschen, wie erheblich die Unterschiede zwischen den beiden Wirtschaftsgütern ihrem Wesen und ihrem Ursprung nach sind. Daten sind im Gegensatz zu jeder anderen natürlichen Ressource potenziell unbegrenzt vorhanden und unter nur geringem Aufwand reproduzierbar. Erst dieser Umstand macht ‚*Big Data*' überhaupt erforderlich: Also die inflationär zunehmende, automatisierte Verarbeitung und Auswertung riesiger Datenbestände, die so groß, schnelllebig oder komplex sind, dass sie sich mittels herkömmlicher Methoden nicht oder nur schwer verarbeiten lassen.

Des Weiteren haben wirtschaftlich relevante Daten eine gänzlich andere Quelle: Nicht tiefere Erdschichten sind ihr Ursprung, sondern ganz regelmäßig einzelne Personen. Damit ist ihr Nutzen nicht ohne Weiteres gegeben. Erst durch die Zuordnung zu bestimmten Akteuren gewinnen sie an Wert. Und so kommen wir der Bedeutung des Datenschutzes schon recht nahe: Den öffentlichen, wirtschaftlichen und staatlichen Interessen an der Erhebung und -verwertung von Daten als Informationsgrundlage stehen stets die Schutzinteressen betroffener Individuen gegenüber. Letztere sehen sich immer größeren Bedrohungen ausgesetzt.

Unter dem Stichwort ‚*Gläserner Mensch*' wird ein Phänomen umschrieben, welches auf der (freiwilligen oder unfreiwilligen) Preisgabe persönlicher Daten basiert und im Extremfall zu einer gänzlichen Aufgabe der Privatsphäre durch völlige Transparentmachung gegenüber Dritten führen kann. Eine Gefahr, die bereits *George Orwell* in den vierziger Jahren zu *1984* und kurz zuvor *Aldous Huxley* zu *Brave New World* inspirierte.

Im Ergebnis stehen sich also zwei Positionen gegenüber: das Schutzinteresse Einzelner an ihrer Privatsphäre und die umfassenden Datenverwertungsinteressen Dritter. Diese miteinander in einen Ausgleich zu bringen, ist, sehr verallgemeinert, Aufgabe des deutschen und europäischen Datenschutzrechts.

So weit, so gut. Doch was sind Daten eigentlich konkret? Und was genau wird rechtlich geschützt? Und vor was?

A. Big Brother is watching you – Zum Gegenstand des deutschen und europäischen Datenschutzes

Art. 1 DSGVO

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

[…]

I. Big Brother is watching - what? Zum Begriff der Daten

Der Jurist und ehem. US-Supreme-Court-Richter *Potter Stewart* schrieb 1964 ein kleines Stück Rechtsgeschichte, als er im Verfahren *Jacobellis v. Ohio* hinsichtlich

der unklaren Definition von Pornografie trocken vermerkte: „I *know it when I see it.*“ Zumindest im Alltagsgebrauch kann dies auch für den Begriff der Daten gelten. Ein Rechtsgebeit kommt jedoch nur schlecht ohne eine konkrete Vorstellung seines Schutzgegenstands aus. Insoweit stellt sich zunächst juristisch die – in der Beantwortung sehr unjuristische – Frage: Was sind Daten?

Art. 4 Nr. 1 der europäischen Datenschutzverordnung (EU-DSGVO) beschreibt den der Verordnung zugrunde gelegten Datenbegriff schlicht als „Information“. Bis in die 2000er Jahre hinein gab es dabei in kaum einer wissenschaftlichen Disziplin eine taugliche Differenzierung zwischen „*Information*“ und „*Daten*“. Auch die Abgrenzung zur „*Mitteilung*” bereitet Schwierigkeiten. Versuchen wir uns also an einer Eingrenzung.

Der US-amerikanische Mathematiker *Claude Shannon* begründete 1948 die naturwissenschaftliche Informationstheorie, als er Informationen als bloße „*Menge von Bits ohne Bedeutung*” definierte – also als bloßes technisches Signal. Nach diesem Verständnis fällt eine Differenzierung zu „Daten” in der Tat schwer, meint auch der italienische Philosoph *Luciano Floridi*. Für ihn sind Informationen, ganz im Gegenteil, „*Daten mit Bedeutung*”, wobei Daten per se eine Erfassung bzw. Kenntlichmachung irgendeines Unterschieds seien. Dieser Unterschied könne im Anschluss mittels Interpretation erkannt werden.

Die Bedeutung der Unterscheidungskraft legte zwar auch *Gregory Bateson* seinem Informationsbegriff zugrunde - ein taugliches Abgrenzungskriterium liefert *Floridi* aber mit der Verbindung zu einer davon losgelösten, eigenständigen Aus- und Bewertung, welche erst aus Daten Information werden lässt.

Nehmen wir als Beispiel meine persönliche Anschrift. Nach *Shannon* müsste diese erst in irgendein Kommunikationssystem eingespeist werden, um dann – losgelöst von jeglicher Zuordnung – sofort als Information gelten zu dürfen. Folgt man Floridi, besteht meine Adresse zunächst aus mehreren Daten, also Unterscheidungsmerkmalen: der Ort in Abgrenzung zu anderen Gemeinden, die Straße zur Orientierung innerhalb des Ortes und die Hausnummer zur genauen Fixierung. Erst durch die Deutung dieser Fragmente entsteht eine verwertbare Information: „Hier scheint der Autor seinen Wohnsitz zu haben. Hier kann er postalisch erreicht werden.” Dabei ist die Interpretation deutlich fehleranfälliger als die Ausgangsdaten selbst. Schließlich könnte die von mir angegebene Anschrift bloße Meldeadresse sein, während ich mich tatsächlich längst auf die Malediven abgesetzt habe.

Nach *Brian Ballson-Stantun* können Daten weiter differenziert werden in:

- ***Facts*** objektive, reproduzierbare Ergebnisse von Messungen, die wahre Aussagen über die Realität liefern, z.B. Temperaturmessungen, Masse der Erde oder die Anzahl an Türen innerhalb eines Gebäudes

- ***Observations*** aufgezeichnete Wahrnehmungen; prinzipiell subjektiv, benötigen Kontextwissen und müssen gefiltert werden, um aus ihnen relevante Informationen zu ziehen, z.B. Audio- und Videoaufnahmen, Notizen eines Künstlers

- ***Bits*** Zeichen, die der Kommunikation dienen: Texte, Diagramme, Tabellen

Sie sind folglich stets Mitteilungen mit teils mehr, teils weniger mittelbarem Informationsgehalt. Und hier schließt sich der Kreis: Schon der Soziologe *Niklas Luhmann* bemerkte, dass aus Mitteilungen erst durch die Komponente des „Verstehens“ eine Information mit Informationswert hervorgehe. Kehren wir zurück zum Recht. Wie angerissen, schützt das deutsche und europäische Datenschutzrecht *personenbezogene* Daten - also v.a. *observations* (z.B. Bewegungsprofile) und *facts* (z.B. Gewicht). Durch den Personenbezug wird deutlich, dass Daten wenigstens zugeordnet und grundsätzlich auch interpretiert werden müssen, um *bezogen auf die Person* Aussagekraft entfalten zu können. Einigen wir uns also auf folgende datenschutzrechtliche Formel: Daten = Mitteilungsfähige Unterscheidungsmerkmale, aus denen durch Verarbeitung (d. h. Filterung, Zuordnung, Speicherung, Auswertung und Interpretation) vollständige oder gänzlich neue Informationen gewonnen werden können.

II. Big Brother is watching YOU! Der Personenbezug

Um den somit eröffneten, sehr weiten Schutzraum etwas einzugrenzen, werden vom Datenschutzrecht nur solche Daten mit Bezug zu identifizierten oder identifizierbaren natürlichen Personen erfasst. Im Gegensatz zur reinen Daten*sicherung*, welche alle Daten selbst vor Verlust, unbefugtem Zugriff oder Fälschung bewahren soll. Es geht dem Daten*schutz* also primär um die Grund- und Persönlichkeitsrechte des dahinterstehenden Menschen.

Dies ist umso wichtiger, weil nach geltendem Recht mangels Körperlichkeit und Rechtscharakter kein Eigentum an Daten bestehen kann, und somit auch keine Eigentumsrechte geltend gemacht werden können. Es bedarf folglich eines besonderen Rechtsregimes, um das Recht auf Privatsphäre oder informationelle Selbstbestimmung bezogen auf personenbezogene Daten gewährleisten zu können.

III. And how does Big Brother do so? Die Datenverarbeitung

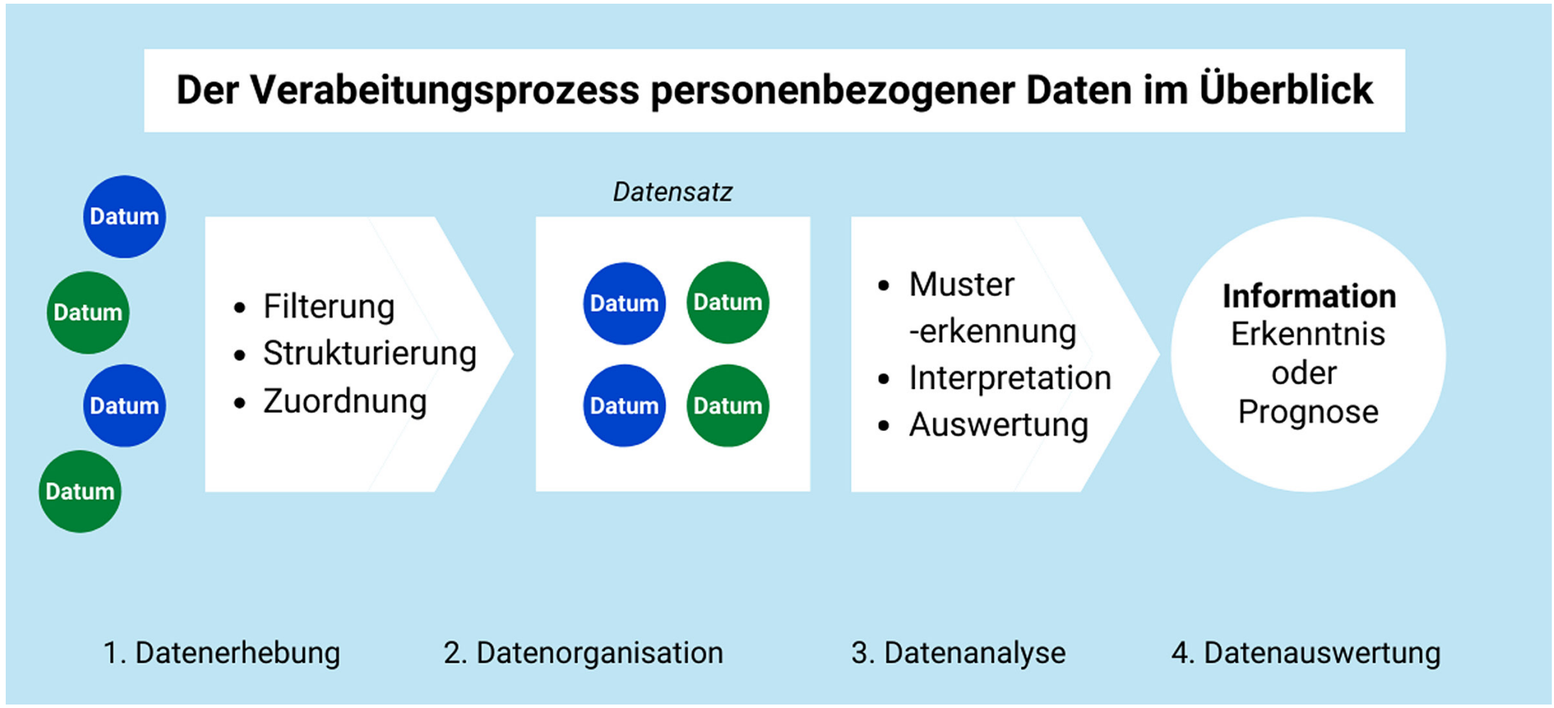
Wie festgestellt, ist ein irgendwie gearteter Verarbeitungsprozess erforderlich, um aus personenbezogenen Daten brauchbare Information gewinnen zu können.

Der europäische und deutsche Datenschutz setzen ebenda an, wobei Art. 4 Nr. 2 DSGVO und § 46 Nr. 2 Bundesdatenschutzgesetz (BDSG) richtigerweise von einem denkbar weiten Verarbeitungsbegriff ausgehen: Von der Erhebung über das Organisieren, Speichern und Auslesen von Daten bis hin zu ihrer Änderung, Weitergabe und Vernichtung wird jeder – mit oder ohne Hilfe automatisierter Verfahren bewerkstelligte – Vorgang erfasst.

Entsprechend dem *Moore*'schen Gesetz, demzufolge Computer von Jahr zu Jahr exponentiell leistungsfähiger werden, haben sich die Herausforderungen des Datenschutzes dabei unlängst verlagert. Es sind bei weitem nicht mehr nur Fragen der Erfassung und Speicherung, die Sorge bereiten. Dank der enormen Menge an verwertbaren Datensätzen und lernenden Algorithmen können aus Daten auch Informationen abgeleitet werden, die gefährliche Möglichkeiten eröffnen. Der Skandal um die britische Firma *Cambridge Analytica* gab auch der breiteren Öffentlichkeit hierfür erste wichtige Einblicke:

Voraussetzungen des Personenbezugs

Das Datenanalyse-Unternehmen sammelte zwischen 2014 und 2018 riesige Mengen an Daten über Millionen von *Facebook*-Usern, um mittels stochastischer Modelle psychologische Profile erstellen zu können. Allein durch Mustererkennung konnten



Der Verarbeitungsprozess personenbezogener Daten im Überblick

so erschreckend präzise Aussagen über höchstpersönliche Eigenschaften einzelner Personen, wie die politische Gesinnung, die sexuelle Orientierung oder auch die mentale Gesundheit, getroffen werden. Und noch bedenklicher: Auch künftiges Verhalten konnte treffsicher prognostiziert werden.

Cambridge Analytica nutzte dies, um zielgruppenspezifische Werbung erstellen zu können. Welche weitreichenden Möglichkeiten für moderne Überwachungsstaaten, potente Unternehmen oder auch Privatpersonen dank neuartiger Formen der Datenverwertung bereits heute bestehen, lässt sich dabei nur erahnen.

B. Der Datensouverän: Die Kernaufgaben des Datenschutzes

Bereits 1890 definierten die US-amerikanischen Rechtswissenschaftler *Samuel Warren* und *Louis Brandeis* in einem aufsehenerregende Aufsatz das „*Right to Privacy*“ als „*Right to be let alone*“. Im Lichte der aufkommenden Fotografie und eines immer sensationsgierigeren Zeitungswesens leiteten die Autoren aus dem anerkannten Recht auf Leben und Eigentum die Notwendigkeit eines besonderen Schutzrechts ab, welches präventiv die Beeinträchtigung der höchstpersönlichen Privatsphäre schützen soll. Tatsächlich war es auch der US-Kongress, der ein halbes Jahrhundert später die ersten datenschutzrechtlichen Ideen diskutierte. Doch das deutsche Bundesland Hessen war es, dass 1970 das weltweit erste Datenschutzgesetz erließ. Der Datenschutz als besondere Ausprägung des Persönlichkeitsrechts hat weniger die Daten als solche als vielmehr die natürliche Person zum Gegenstand, auf die sie sich beziehen. Das hat das Bundesverfassungsgericht schon 1983 in seinem Volkszählungsurteil aus Art. 1 I i.V.m. 2 I GG abgeleitet. Art. 7 und 8 der europäischen Grundrechtecharta erkennen das Recht auf Privatsphäre und den Schutz der persönlichen Daten ausdrücklich als Grundrecht an. Dies soll am besten gewährleistet werden können, indem jedem Einzelnen weitestgehende Selbstbestimmung über

> „Privacy is not something that I‘m merely entitled to, it‘s an absolute prerequisite.“
>
> **Marlon Brando (1960)**

die eigenen Informationen eingeräumt wird. Dieses Prinzip lag bereits den ersten deutschen und europäischen Regulierungen zugrunde - und wird bis heute fortgeführt. Gleichzeitig sollten all die berechtigten Interessen der Allgemeinheit an einem freien, ungestörten und grenzübergreifenden Datenverkehr berücksichtigt werden. Ein schwieriger Ausgleich, schon im Rahmen der ersten europäischen Datenschutzrichtlinie von 1995. Weit weg aber waren damals noch all jene Probleme, die den Datenschutz heute herausfordern. Einerseits können durch immer mehr technischen Fortschritt immer schneller immer größer werdende Datenbestände verarbeitet und weltweit verteilt werden. Dem daraus folgendem Erkenntnisgewinn sind dabei keine Grenzen mehr gesetzt. Der *‚gläserne Bürger'* gibt nicht mehr bloß Angaben über sich Preis: Er weiß mittlerweile gar nicht mehr genau, welche und wie viele Informationen über ihn, von wem, aus scheinbar belanglosen Daten abgeleitet werden können, und an wen diese weitergegeben werden. Die Enthüllungen des ehemaligen NSA-Mitarbeiters *Edward Snowden* sowie der bereits erwähnte *Cambridge-Analytica*-Skandal haben aufgezeigt, dass es sich hierbei längst nicht mehr nur um dystopische Albträume handelt. Andererseits ist der hochfrequente und ungehemmte Datenverkehr heutzutage so relevant wie nie zuvor. Der Austausch von Informationen zwecks Innovation und Wissenschaft, der reibungslose, transnationale Geschäftsverkehr sowie globale Wertschöpfungsketten hängen maßgeblich von ihm ab. So oder so stellt der Ausgleich dieser Interessen als Kernaufgabe des Datenschutzrechts eine enorme Herausforderung dar.

Weiterführende Hinweise:

Zur allgemeinen herausragenden ökonomischen Bedeutung von Daten, ihren marktwirtschaftlichen und wettbewerblichen Implikationen sowie den verblüffenden Parallelen zum Rohstoff Öl vgl. *Haucap*, *Justus*: „Competition and Competition Policy in a Data-Driven Economy.“, (2019), hier abrufbar (Stand: 29.12.2021) sowie

Eppelmann, *Hendrik*: „Big-Tech und Kartellrecht: Regulierungsansätze der EU und in Deutschland.”, CTRL 2/21, 123 ff., hier abrufbar (Stand: 29.12.2021).

Zur Entwicklung des Datenbegriffs und seinen informationstheoretischen und philosophischen Grundlagen vgl. *Voß*, *Jakob*: „Was sind eigentlich Daten?”, (2012), hier abrufbar (Stand: 29.12.2021)

Zu den Auswirkungen von Big Data auf den Schutz der Privatsphäre anhand konkreter Beispiele, vgl. *Steinebach*/*Halvani*/*Schäfer*/*Winter*/*Yannikos*: „Begleitpapier Bürgerdialog. Chancen durch Big Data und die Frage des Privatsphärenschutzes.”, (2014), hier abrufbar (Stand: 29.12.2021)

Und schließlich gibt auch *Warrens* und *Brandeis'* erster Artikel zum „Right to Privacy” interessante Denkanstöße für die rechtliche Bewertung, vgl. Warren/Brandeis, „The Right to Privacy“ (1890), hier abrufbar (Stand: 29.12.2021)

Talking Legal Tech – Folge 28:

Regulierung & Innovation – Wie lässt sich beides vereinbaren, Martin Ebers?

Zurück zum dynamischen Inhaltsverzeichnis?

Zum dynamischen Inhaltsverzeichnis

1/22

2. Jahrgang, 1. Ausgabe
www.legaltechcologne.de/ctrl

CTRL

Cologne Technology & Law Review

Hier geht es zur ganzen Ausgabe

Dort findest Du in 19 Beiträgen alles von Datenschutz bei Connected Cars über Krypto-Auktionen bis hin zum Artificial Intelligence Act und Legal Tech.

LEGAL TECH LAB COLOGNE