Big Data & Datenschutz

Dr. Georg Huber, Rechtsanwalt
Greiter Pegger Kofler Rechtsanwälte, Innsbruck

Inhaltsübersicht

I. Einleitung

Spätestens seit der Affäre um Cambridge Analytica, bei der Facebook in großem Stil personenbezogene Daten weitergegeben hat und diese Daten im US-Präsidentschaftswahlkampf von Cambridge Analytica zum Versand personalisierter Nachrichten mit spezifisch auf den Empfänger bestimmten Inhalten verwendet wurden, ist das Thema «Big Data» verstärkt in den Fokus der Öffentlichkeit getreten.

Cambridge Analytica hat anschaulich vor Augen geführt, welche Möglichkeiten «Big Data» bietet und wie damit sogar die Grundfesten unserer Demokratien zumindest ins Wanken gebracht werden können.

Der Umgang mit Big Data erfordert daher Regeln. Diese Regeln sollen den Einzelnen, aber auch die Gesellschaft als Ganzes vor dem Missbrauch mit Big Data schützen.

Gleichzeitig bietet Big Data zahlreiche Möglichkeiten, die von großem Nutzen sind. Man denke nur an die verbesserten Forschungsmöglichkeiten in der Medizin.

Ein Instrumentarium des Rechtsstaates, diese beiden Ansätze in Einklang zu bringen, ist das Datenschutzrecht. Es geht vor allem darum, den Einzelnen und sein Recht auf informationelle Selbstbestimmung zu schützen, gleichzeitig aber die Rahmenbedingungen für Big Data Anwendungen festzulegen, um sie zum Vorteil der Gesellschaft einzusetzen.

II. Big Data

1. Definition

Unter Big Data versteht man im Allgemeinen die automatisierte Auswertung riesiger unterschiedlich strukturierter Datenmengen in Echtzeit[1].

Die Wesensmerkmale dieser Auswertung lassen sich mit den drei «Vs» beschreiben: *Volume, Variety* und *Velocity*. Manchmal werden diese drei Vs noch durch weitere ergänzt: *Veracity, Validity* und *Value*.

Volume bezieht sich dabei auf die riesigen Datenmengen, die verarbeitet werden.

Variety steht hingegen für die vielen unterschiedlichen Datenquellen und Datenformate bzw. deren unterschiedliche Struktur (z.B. Bilder, Texte, Datenbankeintragungen), die Big Data Anwendungen bewältigen müssen.

Velocity wiederum beschreibt das Erfordernis, dass IT-Systeme diese unterschiedlichen, großen Datenmengen in Echtzeit verarbeiten müssen. Bei *smart traffic* Anwendungen etwa müssen Verkehrsdaten aus verschiedenen Quellen in Echtzeit erfasst und bearbeitet werden, um Verkehrsströme zu lenken. Es geht dabei z.B. um Fahrzeugdaten, Umgebungsdaten und die Einbettung in smart traffic scenarios.

[1] Vgl. etwa https://de.wikipedia.org/wiki/Big_Data.

Veracity, *Validity* und *Value* beschreiben im Wesentlichen die Datenqualität und den Mehrwert, den Big Data für Unternehmen mit sich bringt. Die Qualität und die Genauigkeit der Daten sind entscheidend dafür, wie zuverlässig und werthaltig Big Data Auswertungen sind. Gerade die Datenqualität variiert oftmals sehr.

Big Data Verarbeitungen gliedern sich grob gesagt in drei Schritte:

(i) Erhebung der Daten,

(ii) die Speicherung und Zusammenführung der Daten und

(iii) die Analyse und der Einsatz der Ergebnisse, z.B. im Rahmen automatisierter Entscheidungsfindungen.

Bei der Datenerhebung geht es hauptsächlich um Fragen des Eigentums an Daten – also wem die Daten gehören und wer sie nutzen darf. Ist dies etwa der Fahrer eines Fahrzeuges, der die Daten während der Fahrt generiert, oder ist es der Eigentümer des Fahrzeuges oder ist es der Hersteller des Fahrzeuges oder vielleicht der Hersteller der Sensoren oder der Auswertungssoftware? Allerdings spielen auch schon bei der Erhebung von Daten Fragen des Datenschutzes eine Rolle, etwa ob die Erhebung grundsätzlich zulässig ist.

Bei der Speicherung, Zusammenführung, Analyse und dem Einsatz der Daten stellen sich dann vermehrt datenschutzrechtliche Fragen. Es geht im Wesentlichen um die Zulässigkeit dieser Prozesse und den Schutz der Betroffenen.

2. Datenherkunft und Nutzen von Big Data

Schätzungen zufolge verdoppelt sich das weltweite Datenvolumen gegenwärtig alle zwei Jahre und wächst exponentiell an[2]. Wir alle generieren enorme Datenmengen. In Big Data Anwendungen werden nach Schätzung derzeit aber lediglich ca. 12% ausgewertet. Es besteht also noch ein riesiges Potential an Big Data Anwendungen, das allein aufgrund des massiven künftigen Datenzuwachses stetig steigt.

[2] Vgl. etwa www.statista.com

Wo werden nun all diese Daten generiert? Es gibt unzählige Datenquellen, wie z.B.:

- Überwachungssysteme (z.B. Kameras, Sensoren, RFID-Chips)
- Kundendaten (z.B. Kunden-, Bankomat-, Kreditkarten)
- Elektronische Kommunikation/Internet, z.B. Smartphone, SMS, Telefonie, Surfverhalten
- Apps (WhatsApp, GPS, Fitness, Health etc.)
- Social Media
- Internet of Things
- Smart Meters
- Behörden, Geheimdienste
- Gesundheitseinrichtungen

Wir überlassen laufend unseren digitalen Fußabdruck in der virtuellen Welt. Kaum einer von uns, der nicht täglich über Social Media, das Internet, sein Smartphone/Tablet oder anderweitig Daten über sich selbst verbreitet.

Der Wert dieser Daten ist besonders für die Wirtschaft, aber etwa auch für die Forschung, von großem Wert. Algorithmen werten diese Daten aus. Nach Pressemitteilungen kann ein Algorithmus bei 70 Likes auf Facebook den User besser einschätzen als dessen Freunde. 150 Likes und der Algorithmus ist besser als Eltern und mit 300 Likes hat der Lebenspartner gegen die Maschine das Nachsehen. 350 Likes und die Maschine kennt den User besser als er sich selbst[3].

Big Data haben daher für die Wirtschaft, aber auch für die öffentliche Hand (z.B. im Gesundheitswesen) großen Nutzen. Sie erlauben die Verbesserung und Optimierung von Geschäftsprozessen und des Marketings, die Entwicklung neuer Technologien oder von im öffentlichen Interesse gelegenen Zielen (z.B. der Kriminalitätsbekämpfung), in Forschung und Wissenschaft, der Werbung, im Handel, in der Finanz- und Versicherungsbranche, der Landwirtschaft, zur Energieverbrauchssteuerung (Stichwort: smart meter), im Verkehr, der Industrie oder in der Medizin.

[3] *Barbara Grech* in der Tageszeitung «Die Presse», 22. März 2018.

Big Data eröffnet aber auch die Möglichkeit des Missbrauchs. Thilo Weichert, der Schleswig-Holsteinische Datenschutzbeauftragte, drückte dies folgendermaßen aus:

«Big Data eröffnet Möglichkeiten des informationellen Machtmissbrauchs durch Manipulation, Diskriminierung und informationelle ökonomische Ausbeutung – verbunden mit der Verletzung der Grundrechte der Menschen.»[4]

Der Erhebung, Auswertung und Verwendung von Big Data müssen daher Grenzen gesetzt werden. Die Schwierigkeit besteht wohl darin, den schmalen Grat zwischen Verbot und schrankenloser Nutzungsfreiheit zu finden, um sowohl den Einzelnen und die Gesellschaft zu schützen, als auch positive Entwicklungen durch Big Data zu ermöglichen.

III. Datenschutzrechtliche Anknüpfungspunkte

1. Ziele der DSGVO

Die DSGVO gibt in ihrem Art. 1 und den zugehörigen Erwägungsgründen[5] selbst Auskunft über ihre Zielsetzungen (wobei das Ziel der Harmonisierung des Datenschutzes hier außer Acht bleibt).

Demnach soll die DSGVO sowohl die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere deren Grundrecht auf Schutz personenbezogener Daten[6], schützen, als auch den freien Datenverkehr in der Europäischen Union gewährleisten.

Die Zielsetzungen sind also einerseits der Grundrechtsschutz und andererseits die Stärkung des Wirtschaftsstandortes. In ErwG 2 DSGVO werden diese zunächst widersprüchlich erscheinenden Zielsetzungen wie folgt umschrieben:

---

4 www.de.wikipedia.org/wikiBig_Data, abgefragt am 27. April 2018
5 ErwG 1 bis 14.
6 Art. 8 der Charta der Grundrechte der Europäischen Union

Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.

Diese doppelte Zielsetzung – Grundrechtsschutz und Stärkung der Wirtschaft – führt im Bereich von Big Data eben genau zu jener Gratwanderung, die die uferlose Nutzung und Ausbeutung von Big Data verhindern soll, aber gleichzeitig sinnvolle und wirtschaftlich erwünschte Big Data Anwendungen erlauben muss.

Letzteres lässt sich nur bewerkstelligen, wenn der Nutzung von Big Data Schranken gesetzt werden, die Missbrauch und die Verletzung des Rechtes der informationellen Selbstbestimmtheit verhindern.

Datenschutz ist aber nicht das einzige Instrument, um Ungleichgewichte in datenreichen Märkten zu verhindern. Daten stellen *das* Kapital der Zukunft dar. Zugang zu Daten und deren Verwertung in Big Data Anwendungen eröffnet noch nie dagewesene Möglichkeiten der Steuerung und Kontrolle unserer Gesellschaft. Es gilt daher etwa auch im Bereich des Wettbewerbsrechtes effiziente Mechanismen einzusetzen, um Missbrauch und die Konzentration der Daten bei wenigen *global playern* zu verhindern[7].

Im Folgenden wird nur dargestellt, wie die DSGVO versucht, Big Data Anwendungen im Lichte dieses Spagates zwischen wirtschaftlicher Effizienz und Schutz des Einzelnen zu regeln. Die Anknüpfungspunkte der DSGVO für Big Data werden im Folgenden anhand ihrer Grundsätze, der Regelungen zu Profiling und der Besonderheiten für im öffentlichen Interesse gelegenen Archivzwecken, Forschung und Statistik dargestellt.

[7] Vgl. dazu *Viktor Mayer-Schönberger / Thomas Ramge,* Das Digital, 3. Auflage, Berlin 2017, 203 ff.

2. Wesentliche Grundsätze DSGVO

2.1 Rechtmäßigkeit

Die DSGVO erlaubt Datenverarbeitungen nur dann, wenn sie «rechtmäßig» erfolgen. Der Grundsatz lautet also, dass Datenverarbeitungen verboten sind, wenn sie nicht ausdrücklich erlaubt sind. Das gilt auch für Big Data Anwendungen.

Die Erlaubnistatbestände sind in Art. 6 und (für besondere Kategorien personenbezogener Daten; «sensible Daten») in Art. 9 DSGVO festgelegt. Für Big Data Anwendungen kommen insbesondere folgende Rechtmäßigkeitsgründe in Betracht:

- Öffentliches Interesse (inkl. Forschung/Wissenschaft)[8] – Art. 6 Abs. 1 lit. e und Art. 9 Abs. 2 lit. i und j DSGVO
- Rechtliche Verpflichtung – Art. 6 Abs. 1 lit. c und Art. 9 Abs. 2 lit. g
- Einwilligung – Art. 6 Abs. 1 lit. a Art. 9 Abs. 2 lit.b
- Überwiegendes berechtigtes Interesse – Art. 6 Abs. 1 lit. f

Gerade für Unternehmen mit rein kommerziellen Big Data Anwendungen, die keine Pseudo- oder Anonymisierung erlauben (z.B. Big Data Auswertungen für Zwecke des Direktmarketing) ,wird wohl nur der Rechtmäßigkeitsgrund der Einwilligung in Frage kommen.

Die Einwilligung setzt Big Data Anwendungen aber insofern Grenzen, als in ihr insbesondere der Zweck der geplanten Datenverarbeitung hinreichend genau beschrieben sein muss[9]. Das ist oft gar nicht möglich, da bei der Erhebung der Daten vielfach noch nicht feststeht, was mit diesen Daten später einmal passieren soll. Daneben dürfte es oft an der «Freiwilligkeit» der Einwilligung und bei Minderjährigen am notwendigen Alter für die Zustimmung mangeln.

Für Big Data Anwendungen im Bereich von Forschung und Wissenschaft stellt die DSGVO erleichtere Anforderungen an die Einwilligung. In ErwG 33 heißt es dazu:

[8] Vgl. hierzu auch Punkt III.4.
[9] Vgl. dazu Punkt III.2.3

Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen.

Hier wird die Zweckbeschreibung in der Einwilligung aufgeweicht, als nur eine allgemeine Zweckangabe für bestimmte Forschungsbereiche erforderlich ist. Voraussetzung ist jedoch, dass die Forschung nach anerkannten ethischen Standards durchgeführt wird. Als Beispiel für einen anerkannten Standard in der Medizinforschung kann etwa die Helsinki Deklaration der World Medical Association[10] dienen.

Big Data Anwendungen könnten auch auf das überwiegende berechtigte Interesse eines Unternehmens gestützt werden. Dieser Rechtmäßigkeitsgrund gilt jedoch dann nicht, wenn besondere Datenkategorien ausgewertet werden, also z.B. Gesundheitsdaten. Für andere Anwendungen greift dieser Grund nur dann, wenn eine Interessensabwägung ergibt, dass die mit der Anwendung verfolgten Interessen jene der Betroffenen, insbesondere deren Grundrechte- und Grundfreiheiten, überwiegen. Möglichweise wird das in der Regel nur dann der Fall sein, wenn die personenbezogenen Daten anonymisiert wurden. Eine Anonymisierung verunmöglicht aber bei manchen Big Data Anwendungen deren Zielerreichung, so etwa im Bereich des Direktmarketings.

Abgesehen davon ist heute eine absolute Anonymisierung oft nicht mehr möglich, da eine Verknüpfung der anonymisierten Daten mit anderen frei verfügbaren Daten zur Rückführbarkeit der Daten auf bestimmte Personen, also eine Entschlüsselung, ermöglichen kann[11]. Abhilfe könnte dabei wohl

[10] www.wma.net

[11] Beispiel: In Australien wurden Gesundheitsdaten von ca. 3 Mio. Personen anonym ausgewertet. Dennoch gelang es, einzelne Datensätze bestimmten öffentlich bekannten Personen zuzuordnen, indem etwa andere bekannte Daten dieser Personen herangezogen wurden. So waren z.B. die Geburtsdaten der Kinder der betroffenen Personen bekannt, was Rückschlüsse auf Krankenhausaufenthalte ermöglichte.

nur eine künstliche, leichte Veränderung der Daten vor ihrer Verarbeitung bieten, was jedoch wiederum die Qualität der Daten und damit die Ergebnisse der Big Data Analysen beeinträchtigt.

Aus all dem ergibt sich, dass Big Data Anwendungen bereits am Erfordernis der Rechtmäßigkeit scheitern könnten und dass Big Data Anwendungen generell eher dann zulässig sind, wenn der Schutz der Betroffenen durch Anonymisierung gewahrt ist.

2.2 Transparenz

Ein weiterer Grundsatz der DSGVO ist jener der Informiertheit. Betroffene müssen unter anderem auch über den Zweck der Datenverarbeitung hinreichend genau und nicht nur allgemein informiert werden[12].

Ebenso wie bei der Einwilligung kann das Transparenzerfordernis besonders bei der Information über den Zweck Probleme bereiten, da dieser im Zeitpunkt der Datenerhebung oft nicht genau feststeht.

Zusätzliche Transparenzerfordernisse ergeben sich dann, wenn Big Data Anwendungen mit einem Profiling und/oder einer automatisierten Entscheidungsfindung verknüpft werden. Die Betroffenen sind über das Profiling samt dessen Folgen hinzuweisen[13].

Im Falle einer automatisierten Entscheidungsfindung sind außerdem Aussagen über die involvierte Logik und deren Tragweite bereit zu stellen. Das könnte im Einzelfall Schwierigkeit bereiten, man denke nur an komplexe Algorithmen, deren Logik wohl nur schwer in einer einfachen und klaren Sprache – wie es die DSGVO erfordert – beschreibbar sein wird.

[12] Vgl. dazu WP260 Transparency Guidelines
[13] Art. 13 DSGVO, ErwG 60

2.3 Zweckbindung und Datenminimierung

Die wesentlichste Einschränkung für Big Data Anwendungen dürfte der Grundsatz der Zweckbindung, verbunden mit jenem der Datenminimierung mit sich bringen.

Der Zweckbindungsgrundsatz hat zwei Ausprägungen: Zum einen die «Zweckfestlegung» und zum anderen die «Zwecknutzung».

Zweckfestlegung bedeutet, dass bereits bei der Datenerhebung der Zweck der geplanten Verarbeitung eindeutig beschrieben werden muss. Der Zweck muss rechtmäßig sein. Wie bereits oben erwähnt reichen allgemeine Zweckfestlegungen nicht. Es bedarf konkreter Beschreibungen. Eine Zweckfestlegung wie «Marketingzwecke» oder «Erhöhung der IT-Sicherheit» genügen diesen Anforderungen nicht[14].

Zwecknutzung wiederum bedeutet, dass später die Daten nicht für Zwecke verarbeitet werden dürfen, die mit dem ursprünglich festgelegten Zweck inkompatibel sind.

Aus dem folgt, dass die Zweckfestlegung zum Maßstab von Datenverarbeitungen wird. Es dürfen nur solche Daten erhoben und genutzt werden, die für die Erreichung des festgelegten Zwecks angemessen, erheblich und notwendig sind. Gerade bei Big Data Anwendungen werden aber oft zahlreiche Daten erhoben, bei denen noch nicht feststeht, wofür sie später überhaupt eingesetzt werden.

Zweckbindung und Datenminimierung verbieten daher eine «Vorratsdatenspeicherung» für allfällige spätere, noch unbekannte Big Data Anwendungen.

Eine Ausnahme besteht lediglich für Archivzwecke, statistische, wissenschaftliche oder historische Zwecke.

Abweichungen vom Grundsatz der Zwecknutzung sind nur im engen Rahmen des Art. 6 Abs. 4 DSGVO möglich. Eine abweichende Nutzung darf

[14] Vgl. dazu WP203 Purpose Limitation

danach nicht «inkompatibel» mit dem ursprünglichen Zweck sein. Für die «Inkompatibilität» sind folgende Kriterien zu berücksichtigen[15]:

- der Zusammenhang mit dem ursprünglichen Zweck («absehbarer nächster Schritt»),
- der Kontext der Datenerhebung,
- die Datenart (z.B. besondere Datenkategorien),
- die Folgen der Weiterverarbeitung und
- die Sicherheiten und Garantien zum Schutz der Betroffenen (z.B. Anonymisierung).

Damit sind jedenfalls eine Auswertung zu gänzlich anderen Zwecken als den ursprünglichen verboten, auch wenn sich z.B. aufgrund technischer Möglichkeiten oder wirtschaftlicher Anforderungen neue Nutzungsmöglichkeiten und Analyseverfahren für bereits vorhande Daten ergeben würden.

Der Zweckbindungsgrundsatz dürfte damit eines der gravierendsten Hindernisse für Unternehmen beim Einsatz von Big Data Anwendungen darstellen.

3. Profiling

Profiling bedeutet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (Art. 4 Abs. 4 DSGVO).

Big Data Anwendungen werden oft mit Profiling verknüpft, z.B. bei Direktmarketinganwendungen. Auch *Cambridge Analytica* versandte seine politischen Werbebotschaften gezielt an spezifische Personen aufgrund derer spezifischer personenbezogener Daten.

[15] Es geht ausdrücklich nicht um «Kompatibilität», sondern um mangelnde «Inkompatibilität», was einen feinen Unterschied darstellt.

Profiling ist nicht grundsätzlich verboten, es ist jedoch an Bedingungen und Voraussetzungen geknüpft. Im Wesentlichen sind diese folgende:

- Durchführung einer Datenschutz-Folgenabschätzung
- Zulässigkeit nur bei einer Einwilligung oder Vorhandensein einer gesetzlichen Grundlage
- Betroffene haben ein Recht auf Widerspruch
- Hinreichende Transparenz[16]

Bei automatisierten Entscheidungen muss zudem über die Programmlogik und deren Auswirkungen informiert werden und der Betroffen hat das Recht, dass eine natürliche Person die automatisiert getroffene Entscheidung überprüft (Art. 22 DSGVO).

Letzteres wird vor allem beim Einsatz von künstlicher Intelligenz im Zusammenhang mit Big Data Anwendungen bedeutsam werden. Entscheidet etwa bei einer Bank nicht mehr ein Sachbearbeiter, sondern ein «Computer» aufgrund vorhandener persönlicher Daten (z.B. Bonitätsdaten, Einkommens- und Vermögensdaten, Alter etc) über eine Kreditvergabe, hat der Betroffene Anspruch, seinen Standpunkt einer natürlichen Person dazulegen und die Entscheidung anzufechten.

Big Data wird künftig eng mit künstlicher Intelligenz verbunden sein, weshalb die DSGVO speziell hier Betroffene schützen muss.

4. Wissenschaft und Forschung, Statistik und Archivierung

Kurz vor Inkrafttreten der DSGVO ist in Österreich eine öffentliche Debatte unter dem Schlagwort «Die Regierung will Daten der Bürger für Forschung freigeben» aufgeflammt[17]. Es ging dabei um die Frage, ob die Daten aus der Elektronischen Medizinischen Gesundheitsakte («ELGA») für wissenschaftliche Zwecke und medizinische Forschung verwendet werden dürfen.

[16] Siehe oben Punkt 3.2.2

[17] Vgl. etwa den Artikel in der Tageszeitung «Die Presse» vom 11.04.2018 mit dem Titel «Regierung will Daten der Bürger für Forschung freigeben»: https://diepresse.com/home/innenpolitik/5403675/Regierung-will-Daten-der-Buerger-fuer-Forschung-freigeben

Mit dem Forschungsorganisationsgesetz[18] hat das österreichische Parlament unter Einhaltung bestimmter datenschutzrechtlicher Vorgaben und Garantien (z.B. Pseudonymisierung) die Verwendung der ELGA-Daten für Forschungszwecke erlaubt.

Im Wesentlichen ging es bei der öffentlichen Debatte darum, ob das öffentliche Interesse an medizinische Forschung Big Data Anwendungen, nämlich die wissenschaftliche Auswertung unzähliger Patientendaten, rechtfertigt und unter welchen Bedingungen dies geschehen darf; weiters, ob die personenbezogenen Daten der Patienten hinreichend geschützt sind.

Unzweifelhaft dürfte gerade bei medizinischer Forschung zur Gewinnung von Erkenntnissen, die der Verbesserung des Gesundheitswesens und der Medizin dienen, ein öffentliches Interesse vorliegen.

Art. 89 DSGVO erlaubt daher eine Datenverarbeitung im öffentlichen Interesse zu Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken. Voraussetzung ist jedoch, dass hinreichend Garantien für die Rechte und Freiheiten betroffener Personen getroffen werden. Der Gesetzgeber kann zur Erleichterung gewisse Ausnahmen von Betroffenenrechten bei solchen Verarbeitungen vorsehen, z.B. vom Auskunftsrecht und auch vom Widerspruchsrecht.

Wesentlich ist auch, dass der Zweckbindungsgrundsatz solchen Verarbeitungen nicht entgegensteht (Art. 5 Abs. 1 lit. b Halbsatz 2 DSGVO). Dies stellt eine gravierende Erleichterung für Big Data Anwendungen im öffentlichen Interesse dar.

[18] BGBl. Nr. 341/1981 zuletzt geändert durch BGBl. I Nr. 31/2018.

IV. Fazit

Der Datenschutz stellt eine der rechtlichen Maßnahmen dar, um Big Data Anwendungen zu regulieren. Daten sind das «neue Kapital» in der Wirtschaft[19]. Es besteht generell die Gefahr, dass Daten aus unterschiedlichen Motiven missbräuchlich verwendet werden. Die heutigen und künftigen technischen Möglichkeiten umfassender und schneller Datenanalysen gepaart mit künstlicher Intelligenz scheinen geradezu zu Missbrauch einzuladen (siehe Cambrigde Analytica).

Neben dem Datenschutz gibt es auch andere rechtliche Instrumentarien zur Regulierung datenreiche Märkte. Das Wettbewerbsrecht ist ebenfalls aufgerufen, dem Missbrauch von Daten, etwa aufgrund einer marktbeherrschenden Stellung, vorzubeugen.[20]

Big Data Anwendungen bringen aber auch ökonomische Vorteile mit sich, weshalb jegliche Regulierung angemessen und auf ein effizientes Gleichgewicht zwischen Schutz der Grundrechte bzw. Grundfreiheiten und den unternehmerischen Freiheiten abstellen muss.

Big Data Anwendungen sind daher nach der DSGVO nicht per se verboten. Sie unterliegen nur Beschränkungen, die teilweise jedoch reicht weitgehend sind.

Das größte Hindernis für Big Data Anwendungen stellt vermutlich der Zweckbindungsgrundsatz dar. Oftmals ist bei der Datenerhebung eine genaue Zweckfestlegung nicht möglich. Daten, die einmal erhoben wurden, dürfen nur für die bei Erhebung festgelegten legitimen Zwecke verwendet werden. Eine Verarbeitung zu anderen Zwecken ist nur in begrenzten Fällen zulässig.

In vielen Fällen wird auch die vorherige informierte Einwilligung der Betroffenen erforderlich sein. Diese bedingt wiederum Freiwilligkeit und eine

[19] Vgl. dazu *Viktor Mayer-Schönberger / Thomas Ramge,* Das Digital, 3. Auflage, Berlin 2017.

[20] Man denke etwa an die großen Unternehmen wie Facebook, Google, Apple, Microsoft etc., die bereits jetzt über riesige Datenmengen verfügen und aufgrund ihrer überragenden Marktstellung diese zum Nachteil der übrigen Marktteilnehmer und der Betroffenen nutzen könn(t)en.

exakte Zweckbeschreibung. Auch daran dürften einige Big Data Anwendungen scheitern.

Generell gilt, dass Big Data Anwendungen mit anonymisierten Daten, wenngleich diese unter Umständen entschlüsselt werden könnten, eher zulässig sind, als andere Big Data Anwendungen. Nicht alle Big Data Auswertungen können anonymisiert erfolgen, da sonst ihr Sinn nicht erfüllt würde, wie z.B. Direktmarketingmaßnahmen.

Für Zwecke der im öffentlichen Interesse gelegenen Archivierung, Statistik, wissenschaftlichen und historischen Forschung bestehen Erleichterungen, insbesondere sind Ausnahmen von den Betroffenenrechten und dem Zweckbindungsgrundsatz vorgesehen.

Es wird sich aber erst in Praxis zeigen, ob die Regelungen der DSGVO praktikabel und geeignet sind, die angestrebten Ziele zu erreichen.

Literatur

Nikolaus Forgó, Stefanie Hänold und Benjamin Schütze, The Principle of Purpose Limitation and Big Data, in: *Marcelo Corrales/Mark Fenwick/Nikolaus Forgó* (editors), New Technology, Big Data and the Law, Singapore: Springer 2017

Rainer Knyrim, Big Data: Datenschutzrechtliche Lösungsansätze, Dako 3/2015

Thomas Helbing, Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 3/2015

Viktor Mayer-Schönberger/Thomas Ramge, Das Digital, Berlin 2017