Wem gehören (digitale) Daten?

Wir gehen selbstverständlich davon aus, dass alles was einen Wert hat auch jemanden gehört/sich im Eigentum von jemanden befindet. Bei Sachen, also körperlichen Gegenständen im Sinne von § 90 BGB, ist das in den allermeisten Fällen auch richtig. Denn andernfalls hätte es nicht der in § 903 Satz 1 BGB wiederzufindenden Regelung bedurft, dass der Eigentümer einer Sache, soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen kann. Doch wie ist das bei „Gegenständen", die man nicht anfassen kann? Es wird zumindest heute kein Zweifel mehr daran bestehen, dass Daten einen sehr hohen Wert haben können. Ein paar der wertvollsten Firmen der Welt (zum Beispiel Google oder Facebook) haben den Grundstein für ihren wirtschaftlichen Erfolg damit gelegt, dass sie insbesondere von Privatpersonen alle möglichen Daten sammeln, um deren Einkaufsgewohnheiten zu analysieren. Die so gewonnenen Profile von Privatpersonen „verkaufen" diese Firmen an Werbekunden, damit diese weniger Streuverluste bei der Schaltung von Werbung haben (eine nette Persiflage zu diesem Thema kann man hier finden). Doch auch über den Bereich der Werbung hinaus haben (auch nicht personenbezogene) Daten bereits heute einen hohen Wert und dieser dürfte zukünftig noch zunehmen. In diesem Zusammenhang soll beispielhaft nur auf die von Maschinen generierten Daten der sogenannten Industrie 4.0 im Zusammenhang mit dem Internet of Things (IoT) verwiesen werden. Hier wird sich zum Beispiel zunehmend die Frage stellen, wer die von den smarten Maschinen generierten Daten nutzen darf. Der Hersteller, der Betreiber/Eigentümer der Maschinen, der Lieferant der Software oder ein sonstiger Dritter?

Was sind eigentlich Daten im rechtlichen Sinne?

Bevor man sich über den rechtlichen Schutz von (digitalen) Daten Gedanken machen kann, muss man zunächst definieren, was man unter Daten versteht.

Allerdings gibt es keine einheitliche gesetzliche Definition, die für alle Rechtsbereiche Geltung beanspruchen kann. § 202a Abs. 2 StGB (Strafgesetzbuch) definiert die über die Straftatbestände der §§ 202a Abs. 1, 303a Abs. 1 StGB geschützten Daten wie folgt: „Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden." Demgegenüber definiert § 312d Abs. 3 BGB digitale Daten folgendermaßen: „Bei Verträgen über die Lieferung von nicht auf einem körperlichen Datenträger befindlichen Daten, die in digitaler Form hergestellt und bereitgestellt werden (digitale Inhalte), ist …". Für die jeweiligen gesetzlichen Zwecke mögen diese Definitionen ausreichend sein. In der juristischen Literatur werden zur Beantwortung der Fragen, wie digitale Daten bereits jetzt geschützt werden und ob der Gesetzgeber darüber hinaus weitere Schutzmechanismen vorsehen muss, die folgenden Unterscheidungskriterien für digitale „Datenarten" für maßgeblich erachtet (z.B. Heymann, CR 2016, 650; Zech CR 2015, 137):

- Semantischen Informationen: Hierbei geht es um den Bedeutungsinhalt von Daten, also um die Informationen, die eine Person über einen Datensatz für sich selbst oder Dritte festhalten will (zum Beispiel den Inhalt eines Gedichts).

- Syntaktische Informationen: Hiermit sind die Informationen eines Datensatzes gemeint, die der Mensch nicht bzw. nicht ohne weiteres lesen kann, weil sie regelmäßig im binären Code verfasst und deshalb nur für Computer zu verstehen sind.

Zumindest für digitale Daten wird für die rechtliche Betrachtung der Frage wem Daten gehören, der syntaktische Informationsgehalt wesentlich sein, denn dieser beinhaltet im Zweifel auch den semantischen Informationsgehalt eines Datensatzes.

Daten sind keine Sachen und deshalb gibt es kein Eigentum an Daten!

In einem kürzlich veröffentlichten Urteil vom 21. September 2017 hat der Bundesgerichtshof im Zusammenhang mit zwangsvollstreckungsrechtlichen Fragen kurz und knapp festgestellt, dass es sich bei nicht auf einem geeigneten Datenträger verkörperten Daten nicht um Sachen im Sinne von § 90 BGB handelt (Az. I ZB 8/17, siehe Rn. 15). Damit hat er zugleich bestätigt, was in der juristischen Literatur insoweit auch unumstritten war. Wenn es sich jedoch bei Daten im Allgemeinen und digitalen Daten im Speziellen nicht um Sachen im Sinne von § 90 BGB handelt, dann gibt es auch kein originäres Eigentumsrecht an den Daten und der rechtmäßige Besitzer der Daten kann gegenüber Dritten weder aus § 903 BGB noch aus § 985 BGB gegen „unberechtigte" Dritte vorgehen. Dies stellt eine beträchtliche Schwächung der rechtlichen Position des Schaffers und/oder des rechtmäßigen Besitzers von Daten dar. Insoweit muss man sich die Frage stellen, ob die Besitzer von Daten völlig rechtlos gestellt sind?

Es gibt eine Vielzahl von Normen aus verschiedenen Rechtsbereichen, die dem Berechtigten Besitzer von Daten einen lückenhaften Schutz gewähren. Zumindest in einem Urteil vom 10. Juli 2015 hat ein anderer Senat des Bundesgerichtshof (Az.: V ZR 206/14, siehe Rn. 20) vorausgesetzt, dass es bei digitalen Daten einen alleinigen Berechtigten geben kann. Der Bundesgerichtshof hat dazu ausgeführt:

> „… Entschließt er sich etwa dazu, dieselben Inhalte nicht auf einem eigenen Tonband zu speichern, sondern beispielsweise auf einen über das Internet zugänglichen Speicherplatz in einem entfernten Rechenzentrum (sogenannte Cloud), bleibt er weiterhin alleiniger Berechtigter der gespeicherten Inhalte. …"

Allerdings lässt dieses Urteil jedwede verwertbaren Ausführungen dazu vermissen, aus welcher Rechtsgrundlage sich im angeführten Beispiel der Status als alleiniger Berechtigter ableiten lässt.

Nachfolgend soll kurz dargestellt werden, wie Daten bereits jetzt rechtlich geschützt werden. Wer sich vertieft mit dieser Fragestellung befassen möchte, kann u.a. die folgenden Aufsätze als Ausgangspunkt dafür nehmen:

- Grützmacher, CR 2016, 485 ff.: Dateneigentum – ein Flickenteppich …
- Heymann, CR 2016, 650 ff.: Rechte an Daten
- Zech, CR 2015, 137 ff.: Daten als Wirtschaftsgut …
- Dorner, CR 2014, 617 ff.: Big Data und „Dateneigentum" …

Das Datenschutzrecht (BDSG und DSGVO)

Schutzgut des Datenschutzrechts sind nur personenbezogene Daten. Gemäß § 3 Abs. 1 BDSG in der bis zum 25. Mai 2018 geltenden Fassung sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Das Datenschutzrecht schützt also nur Daten, die einen Bezug zu natürlichen Personen haben. Alle sonstigen Daten, insbesondere von Maschinen ohne Personenbezug erzeugte Daten oder Geschäftsgeheimnisse, werden vom Schutzbereich des Datenschutzrechts nicht erfasst.

Das Urheberrecht (UrhG)

Das Urheberrecht vermittelte dem Erschaffer von geistigen Werken, wie zum Beispiel Gedichten, Büchern, Skulpturen oder auch besonders designten Gebrauchsgegenständen eine eigentümerähnliche Rechtsposition. Das Urheberrecht schützt insofern nicht ganz allgemein Daten im vorgenannten Sinn, sondern nur den semantischen Inhalt von Daten, wenn dieser nach den Regeln des Urheberrechts schutzfähig ist. Unabhängig davon schützt das Urheberrecht jedoch Datenbanken, wenn im Groben die folgenden Voraussetzungen erfüllt sind:

Zum einen werden Datenbanken, also eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit elektronischen Mitteln oder auf andere Weise zugänglich sind (Definition nach Art. 1 Abs. 1 der Richtlinie 96/9/EG), über § 4 Abs. 2 UrhG geschützt, wenn der Auswahl und/oder der Anordnung der gesammelten Daten eine besondere geistige Leistung zugrunde liegt, die über die üblichen (Darstellungs-/Aufbereitungs-)Kriterien hinausragt. Werden diese Anforderungen nicht erfüllt, was häufig der Fall sein wird, dann kann eine Datenbank auch gemäß §§ 87a ff. UrhG Schutz genießen. Das ist der Fall, wenn die Beschaffung, Überprüfung oder Darstellung des Inhalts der Datenbank vom Erschaffer der Datenbank eine wesentliche Investition erfordert hat. Im Gegensatz zu den eigentlichen Schutzgütern des Urheberrechts, nämlich dem Schutz geistiger Leistungen, der sich in einem konkreten Werk manifestiert hat, wird hier „allein" die Investition in den Aufbau der Datenbank geschützt. Und selbst wenn eine Datenbank gemäß §§ 87a ff. UrhG geschützt ist, dann sind nach der Rechtsprechung zur Auslegung des § 87b UrhG Entnahmen aus dieser Datenbank, die einen Umfang von 10 % der Datenbank nicht überschreiten, vom Schutzrechtsinhaber zu akzeptieren (siehe z.B. Bundesgerichtshof, 01. Dezember 2010, Az.; I ZR 196/08). Notwendig ist jedoch in jedem Fall die systematische Zusammenstellung und Anordnung von Daten. Allein aus diesem Umstand wird deutlich, dass nur ein Bruchteil aller verfügbaren Daten tatsächlich in den Schutzbereich der vorgenannten Regelungen fällt. Insbesondere Geschäftsgeheimnisse werden häufig diese Anforderungen nicht erfüllen.

Auch die §§ 69a ff. UrhG werden im Regelfall nicht weiterhelfen, da über diese Regelungen nur Computerprogramme geschützt werden. Die von Computerprogrammen verarbeiteten oder erzeugten Daten werden gerade nicht geschützt. Als Beispiel hierfür kann man zum Beispiel eine Software zum Auswerten von Daten, die unter anderem darauf aufbauend Berichte erstellt, nehmen. Eine solche Software benötigt zum einen Daten, die ausgewertet werden sollen. Diese

Daten sind jedoch nicht Bestandteil des Computerprogramms und werden insofern nicht über §§ 69a ff. UrhG geschützt. Auch der vom Computerprogramm generierte Bericht genießt weder Schutz über §§ 69a ff. UrhG, da es sich hierbei nicht um das Computerprogramm selbst, sondern um ein von ihm generiertes Ergebnis handelt, noch als Datenbank im vorgenannten Sinne, da diese Datenbank, wenn es sich um eine solche handeln sollte, weder von einem Menschen erschaffen noch eine von einem Menschen veranlasste wesentliche Investition zur Erschaffung dieser Datenbank im oben genannten Sinne notwendig wurde.

Das Gesetz gegen den unlauteren Wettbewerb (UWG)

Geschäftsgeheimnisse werden im Wesentlichen über § 17 UWG geschützt. Nach dieser Norm macht sich strafbar, wer die Voraussetzungen in den dort genannten Tatbeständen erfüllt und dadurch die bisher von einem Unternehmen geheim gehaltenen Informationen unbefugt an Dritte weitergibt. Die Schwäche dieser Schutznorm besteht darin, dass Daten, die nicht mehr als geheim im Sinne dieser Vorschrift anzusehen sind, dem Anwendungsbereich der Norm entzogen sind. Wenn vormals geheime Daten also nicht mehr geheim sind, werden sie nicht mehr von dieser Norm geschützt, selbst wenn der „Veröffentlichung" der Daten eine unrechtmäßige Tat zu Grunde lag. Die Abgrenzung, ob Daten noch geheim im Sinne dieser Vorschrift sind, kann im Einzelfall schwierig sein. Regelmäßig wird jedoch nicht mehr von geheimen Daten im Sinne dieser Vorschrift auszugehen sein, wenn diese ohne technische oder sonstige Vorkehrungen für deren Schutz zu treffen, an eine Vielzahl von außerhalb des Unternehmens stehende Personen weitergegeben werden.

Das Strafrecht/Strafgesetzbuch (StGB)

§ 202a Abs. 1 StGB weist eine ähnliche Schutzrichtung wie § 17 UWG auf. Über diese Norm soll das unbefugte Lesen von Daten durch die Überwindung von technischen Sicherungsmechanismen verhindert werden. Im Gegensatz dazu schützt § 303a Abs. 1 StGB die Integrität von digitalen Daten vor der unbefugten

Veränderung durch Dritte. Problematisch ist in diesem Zusammenhang, dass wohl bis heute nicht zweifelsfrei geklärt ist, wie genau die Personen zu ermitteln sind, die von den vorgenannten Strafrechtsnormen geschützt werden. Das Problem kann anhand von in einer Cloud hinterlegten Daten ganz gut beschrieben werden. Es gibt eine Ansicht, die die Meinung vertritt, dass der Eigentümer der jeweiligen Speichermedien geschützt wird. Im Gegensatz dazu vertritt die wohl herrschende Meinung die Ansicht, dass derjenige, der den sogenannten Skripturakt vorgenommen hat, geschützt wird. Unter Skripturakt im diesem Sinne hat man wohl das tatsächliche Speichern der Daten auf dem jeweiligen Datenträger zu verstehen. Dementsprechend würde nach der herrschenden Meinung der Nutzer der Cloud und nicht der Eigentümer des Speichermediums geschützt. Insofern vermitteln diese Strafrechtsnormen dem zur Nutzung der Daten Berechtigten einen relativ weiten Rechtsschutz. Allerdings geben diese Normen keinen wirklichen Aufschluss darüber, wer zivilrechtlich zur Nutzung der Daten berechtigt ist.

§ 823 BGB

§ 823 Abs. 1 BGB gewährt demjenigen, der durch ein schuldhaftes Verhalten eines Dritten einen Schaden an den dort genannten Rechtsgütern erleidet, einen Schadensersatzanspruch gegenüber dem Schädiger. Wenn die vorgenannten Voraussetzungen nicht vorliegen, zum Beispiel weil ein nicht über § 823 Abs. 1 BGB geschütztes Rechtsgut wie das Vermögen des Geschädigten betroffen ist, dann kann dem Geschädigten jedoch gemäß § 823 Abs. 2 BGB in Verbindung mit einem Schutzgesetz, wie zum Beispiel § 303a Abs. 1 StGB, ein Schadenersatzanspruch zustehen. In der alltäglichen Praxis werden die meisten Menschen mit dieser Norm in Berührung gekommen sein, wenn Sie schon einmal einen Unfall erlitten haben. Denn zumeist leitet sich der dann für den Geschädigten maßgebliche Schadensersatzanspruch aus § 823 BGB ab. Im Zusammenspiel mit § 303a Abs. 1 StGB kann also der berechtigte Inhaber von Daten von demjenigen, der seine Daten unbefugt verändert hat, Schadenersatz verlangen. In diesen Fällen dürfte sich jedoch die Bezifferung des Schadens schwierig gestalten, denn der Geschädigte

hat genau darzulegen, aufgrund welcher Umstände ihm in welcher Höhe ein vom Schädiger zu ersetzender Schaden entstanden ist. Dies hört sich einfacher an, als es in der Wirklichkeit ist.

Herausgabeansprüche

Der datenträgerlose Austausch von Daten mit Geschäftspartnern, aber auch die Hinterlegung von Daten auf von Dritten bereitgestellten Speichermedien beherrschen mittlerweile den Geschäftsalltag von vielen Unternehmen. Doch wie kommt der ursprüngliche Inhaber der Daten rechtlich wieder in den (alleinigen) Besitz seiner Daten, wenn die Geschäftsbeziehungen beendet wurden und der Geschäftspartner die Herausgabe verweigert. Etwaige Herausgabeansprüche richten sich grundsätzlich nach der Art des Vertrages, der zwischen den Geschäftspartnern geschlossen wurde. Bei Geschäftsbesorgungen im Sinne von § 675 BGB, also Geschäften bei denen der Datenverwender die Daten im Zusammenhang mit einer Vermögensbetreuungspflicht zugunsten des Inhabers der Daten benutzt, kann sich ein solcher Herausgabeanspruch aus § 667 BGB ergeben. Aufgrund der Tatsache, dass hier eine Vermögensbetreuungspflicht beim Verwender der Daten vorliegen muss, zeigt sich bereits, dass der Anwendungsbereich für diesen Herausgabeanspruchs relativ eng ist.

Sollten die Geschäftspartner unentgeltlich zusammengearbeitet haben, so kann sich der Herausgabeanspruch unmittelbar aus § 667 BGB ergeben. Darüber hinaus kann ein Herausgabeanspruch nicht ganz allgemein auf § 667 BGB gestützt werden.

Im Zusammenhang mit Mietverträgen, also zum Beispiel Verträgen über die Nutzung von Cloud-Speichern, ist umstritten, ob sich ein Herausgabeanspruch zumindest über eine analoge Anwendung des § 539 Abs. 2 BGB herleiten lässt.

Zudem lässt sich in den Fällen, in denen der Berechtigte Inhaber der Daten vom Vertrag zurücktritt, aus § 346 Abs. 1 BGB ein Herausgabeanspruch ableiten. Dieser

wird aber bei der Kündigung eines Dauerschuldverhältnisses auch nicht analog zum Tragen kommen.

Urteile, die sonstige Anspruchsgrundlagen für eine Herausgabe von Daten zum Gegenstand hatten, sind mir jedenfalls bisher nicht bekannt geworden. Insofern wird auch in der juristischen Literatur allgemein festgestellt, dass für den Gesetzgeber im Bereich der Herausgabeansprüche noch ein gewisser Handlungsbedarf besteht. Um Probleme bei der Begründung von Herausgabeansprüchen zu vermeiden, sollten die Vertragspartner genaue Regelungen, die sich mit der Herausgabe und der Löschung von zur Verfügung gestellten Daten beschäftigen, in die jeweiligen Verträge aufnehmen.

Fazit

Es mag überraschen, dass es kein Eigentum an Daten gibt und insofern sowohl die Zuweisung von Verfügungsrechten an Daten, als auch die Geltendmachung von Ansprüchen die im Zusammenhang mit Daten stehen können (zum Beispiel die Herausgabe von Daten) in der Praxis durchaus Schwierigkeiten bereiten kann. Gerade vor dem Hintergrund, dass immer mehr Daten produziert werden und diese Daten auch durchaus einen hohen Marktwert haben, kann man zu Recht die Frage stellen ob der Gesetzgeber hier nicht klare Verhältnisse schaffen muss. Allerdings sind sowohl eine von den Justizministern der Bundesländer eingesetzte Kommission (deren Ergebnisse finden Sie hier), als auch die herrschende Meinung in der juristischen Literatur der Ansicht, dass die Schaffung von Eigentumsrechten an Daten derzeit nicht angezeigt ist, da dadurch gerade hinsichtlich des IoT bzw. der Industrie 4.0 mehr Probleme geschaffen als gelöst würden. Man muss also auf die am Anfang gestellte Frage, wem Daten gehören, antworten, dass dies nicht eindeutig gesetzlich geregelt ist und in absehbarer Zeit nicht damit gerechnet werden kann, dass sich an diesem Zustand etwas ändern wird.

Damit der Dateninhaber gegenüber seinen Vertragspartner „unproblematisch" die Herausgabe von digitalen und nicht auf einem besonderen Datenträger gespeicherten Daten verlangen kann, sollten in jedem Vertrag, der in irgendeiner Weise auch den Austausch von Daten zum Gegenstand hat, Regelungen aufgenommen werden, die die Herausgabe der Daten zumindest im Zeitpunkt der Beendigung des Vertragsverhältnisses regeln. Darüber hinaus sollten diese Regelungen auch Löschungspflichten des Vertragspartners enthalten, denn regelmäßig wird der ursprüngliche Dateninhaber vom Vertragspartner nicht die Herausgabe aller Speichermedien, auf denen die von ihm zur Verfügung gestellten Daten enthalten sind, fordern können. Vielmehr werden sich seine Ansprüche darauf beschränken, eine Herausgabe der Daten, also den Erhalt einer Kopie der bei Vertragspartner gespeicherten Daten zu erlangen und den Vertragspartner dazu zu verpflichten, die vom ursprünglichen Dateninhaber erhaltenen Daten zu löschen. Entsprechende Regelungen müssten zudem Ausnahmen für solche Daten vorsehen, die der Vertragspartner aufgrund von gesetzlichen Aufbewahrungspflichten auch über die Beendigung des Vertrages hinaus noch für einen gewissen Zeitraum vorhalten muss.

Ass. jur. Kai Riefenstahl
28.01.2018