

# Internet of Things, Artificial Intelligence, Edge Computing: «Legal Engineering» für neue digitale Geschäftsmodelle

Die Vernetzung von Gegenständen aller Art («Internet of Things») sowie die Verarbeitung der exponentiell wachsenden Datenmengen durch Algorithmen mit kognitiven Fähigkeiten («Artificial Intelligence») ermöglichen neue digitale Geschäftsmodelle, die noch bis vor kurzer Zeit undenkbar gewesen wären. Die rechtliche Ausgestaltung und Absicherung dieser Geschäftsmodelle erfordert nicht nur juristischen Sachverstand, sondern ein Verständnis für Technologietrends und die damit verbundenen Chancen und Risiken.

## Daten als Treibstoff digitaler Geschäftsmodelle

Im Zentrum digitaler Geschäftsmodelle stehen Daten aller Art. Daten sind flüchtig, einfach multiplizierbar und lassen sich ohne relevanten Zeitverlust rund um die Welt transportieren. Obwohl Daten für den Erfolg neuer Geschäftsmodelle in fast allen Branchen zentral sind, ist ihre Stellung in der Rechtsordnung alles andere als geklärt. Zum Beispiel verwehren sich Daten dem altbewährten rechtlichen Instrument des «Eigentums».

Für den Erfolg digitaler Geschäftsmodelle ist ein Konzept zum Umgang mit regulatorischen Verpflichtungen bei der Erhebung, Speicherung und Bearbeitung von Daten unabdingbar. Dies gilt insbesondere für den Schutz der Privatsphäre beim Umgang mit Personendaten sowie bei der Datensicherheit. Ausserdem wollen Unternehmen ihre Investition in die Gewinnung von Daten absichern. Dies gilt auch (und in immer grösserem Masse) bei von Maschinen generierten Daten ohne Personenbezug.

## Datenschutz im Sinne der DSGVO greift zu kurz

Mit Blick auf das Inkrafttreten der EU-Grundverordnung zum Datenschutz (DSGVO) am 25. Mai 2018 sind viele Unternehmen zur Zeit mit Compliance Projekten für den Umgang mit Personendaten befasst. Dies gilt auch für Unternehmen in der Schweiz, wenn sie in den extraterritorial konzipierten Anwendungsbereich der DSGVO fallen. Inzwischen haben sich bewährte Prozesse herauskristallisiert, deren Anwendung für all jene Unternehmen keine grosse Herausforderung darstellt, die sich schon vorher einem verantwortungsvollen Umgang mit Personendaten sowie hohen Standards bei der IT-Sicherheit verschrieben hatten. Alle anderen Unternehmen haben mit Blick auf die verschärften Regeln (die demnächst grösstenteils auch in das Schweizer Recht Aufnahme finden dürften) noch einiges an Hausaufgaben vor sich.



**Dr. Rolf Auf der Maur**

Rechtsanwalt

Leiter des Praxisbereichs Technologie-  
und Kommunikationsrecht

VISCHER

Man kann sich fragen, ob Datenschutz im Sinne der DSGVO zu einem besseren Schutz der Privatsphäre oder vor allem zu mehr administrativem Aufwand bei der Compliance führt. Real ist auf jeden Fall das Unbehagen vieler Konsumenten und Arbeitnehmer darüber, was mit ihren Daten geschieht. Ungenügende Transparenz im Umgang mit Personendaten kann daher neben hohen Bussen einen Reputationsverlust zur Folge haben. Auch sind bereits erste Unternehmensübernahmen daran gescheitert, dass bei der Due Diligence Prüfung eklatante Mängel im Umgang mit Personendaten festgestellt wurden. In Zukunft sind Unternehmen jedenfalls gut beraten, wenn sie bereits bei der Entwicklung von Produkten und Dienstleistungen dem Prinzip «Privacy by Design» folgen und Datenrechtsspezialisten frühzeitig in den Entwicklungsprozess einbinden.

Aber: Auch Daten ohne Personenbezug können einen grossen Wert für Unternehmen darstellen. Solche liegen allerdings ausserhalb des Anwendungsbereichs der Datenschutzgesetze.

## Kontrolle des Zugangs zu Daten

Weil unsere Rechtsordnung kein «Eigentum» an Daten im herkömmlichen Sinne kennt, sind andere Massnahmen zu treffen, um Investitionen in die Gewinnung von Daten abzusichern. Wer etwa als Hersteller von Haushaltsgeräten oder Fahrzeugen Daten über eingebaute Sensoren erhebt, sollte vertraglich die Vertraulichkeit dieser Daten gegenüber seinen Geschäftspartnern entlang der Wertschöpfungskette sicherstellen.

Besondere Herausforderungen stellen sich dann, wenn ein Unternehmen Daten von den Sensoren direkt zu Applikationen in der Cloud übermittelt und dort analysiert. Wer bspw. Bild- oder Sprachdaten in die von Google betriebene Cloud übermittelt und dort die mit künstlicher Intelligenz arbeitenden Bild- oder Sprachanalyseedienste nutzt, kann mit verhältnismässig geringen Kosten rasch wertvolle Erkenntnisse gewinnen. Den grössten Erkenntnisgewinn erzielt jedoch Google. Deren Algorithmen mit kognitiven Fähigkeiten stehen bei zahlreichen Kunden gleichzeitig im Einsatz. Das ermöglicht es Google, aus den kumulierten Daten aller Kunden zu lernen. Unternehmen stehen also vor der Wahl, selber viel Geld in «Artificial Intelligence» zu investieren oder aber die Dienste einer Plattform wie Google oder Amazon in Anspruch zu nehmen, was mittel- oder langfristig mit dem Verlust ihres Wettbewerbsvorsprungs verbunden sein kann.

## Edge Computing kann Datenhoheit stärken

Wer die erhobenen Daten nicht ungefiltert in die Public Cloud übertragen will, kann mit Hilfe von «Edge Computing» Algorithmen zur Datenanalyse nahe bei der Datenquelle einsetzen. Edge Server oder «Cloudlets» können lokal oder in einer privaten Cloud installiert sein und dort die Rohdaten filtern, analysieren oder mit anderen Daten abgleichen. In die «Public Cloud» gehen dann nur noch diejenigen Daten, die der Zweck der dort betriebenen

Applikationen erfordert. Damit lassen sich die Daten besser schützen. Gleichzeitig erleichtert Edge Computing die Erfüllung der regulatorischen Anforderung der Datenminimierung, weil sich beispielsweise Personendaten bereits an der Quelle anonymisieren und aggregieren lassen. Als positiver Nebeneffekt erhöht Edge Computing auch die Performance von datenreichen «Internet of Things» Applikationen.

## Anspruch auf Zugang zu Daten?

Fragen wirft schliesslich auch das Recht auf Zugang zu Daten auf, wenn diese bspw. durch staatliche Institutionen generiert oder in den Händen grosser Plattformen sind. Bei Daten der öffentlichen Verwaltung wird der Ruf nach Zugang für privatwirtschaftliche Zwecke immer lauter («Open Government Data»). Schwieriger begründen lässt sich die Forderung gegenüber den global agierenden grossen Plattformen wie Google, Amazon, Facebook und Apple. Auch wenn diese aufgrund ihrer enormen Datenmengen eine starke Stellung in immer mehr nachgelagerten Märkten haben, lässt sich mit den herkömmlichen Mitteln des Wettbewerbsrechts kein Anspruch auf Zugang herleiten. Die strategische Positionierung gegenüber diesen auch als «Frenemies» (zusammengesetzt aus den Begriffen «Friend» und «Enemy») bezeichneten Plattformen ist für Unternehmen aus zahlreichen Branchen eine Schicksalsfrage.

Recht und Regulierung brauchen keine Innovationsbremse zu sein. Wenn das Wechselspiel zwischen Innovation und Legal Engineering stimmt, lassen sich meist passende Lösungen entwickeln.

TEXT DR. ROLF AUF DER MAUR

**VISCHER**  
SWISS LAW AND TAX