Datennutzung und Datensicherheit – ungleich lange Spieße für Europa

Ende letzten Jahres hat ein BBC Reporter sich in das chinesische Überwachungssystem eintragen lassen – 7 Minuten hat sein Spaziergang gedauert, bis er von den omnipräsenten Videokameras identifiziert und von der Polizei aufgegriffen wurde. Die US Regierung verlangt von Cloud Anbietern auf im Ausland (z.B. Europa) gespeicherte Daten von Ausländern (Sie/ich) zugreifen zu können (Höchstgerichtsentscheidung steht an). Europa, i.e.S. die EU und auch wir, sehen die Verfügung über die eigenen Daten (also z.B. die Löschung) als demokratisches Grundrecht an.

Wie passt das zusammen und was sind die Konsequenzen für unsere Unternehmen?

Um Fahndungsleistungen wie in China erbringen zu können, müssen die biometrischen Daten der eigenen und ausländischen Bürger beim Staat gespeichert, eine flächendeckende Videoüberwachung etabliert und modernste Gesichtserkennungstechnologie (Thema: Artificial Intelligence) eingesetzt werden. Dazu passt der für wie selbstverständlich akzeptierte Anspruch Chinas über alle Daten seiner Unternehmen verfügen zu können. Auch das am 19. Parteitag der kommunistischen Partei Chinas im Oktober 2017 formulierte Ziel, bis 2020 ein Punktesystem für das Wohlverhalten von Bürgern zu entwickeln, passt in das chinesische Bild der Datennutzung und des Datenschutzes.

Die Idee, die eigenen Daten zentral löschen zu lassen, wie die Idee, den Zugriff auf die eigenen Daten selbst bestimmen zu können, passt damit allerdings nicht zusammen. Damit müssen wir uns auch Sorgen machen, dass chinesische Unternehmen, die europäische kaufen (wie deutsche Mittelständler, skandinavische Autoproduzenten oder EU Banken und Kartenanbieter), Daten postwendend an den chinesischen Staat liefern. Chinesische Unternehmen, die in Europa Geschäfte machen (wie Alibaba oder Fahrradverleiher), könnten diese Daten ohne europäische Datenschutzgedanken (siehe EU-Datenschutzverordnung) bereits jetzt verwenden. Europa müsste das kontrollieren und Reziprozität von China verlangen können. Wahrscheinlich ist das eine Illusion.

Fakt ist, Clouds sind im Aufschwung: Zentrale Softwarewartung, Software mieten statt kaufen, praktisch unbegrenzter Speicherplatz, aber auch der zentrale Datenschutz, garantiert von den besten Köpfen der Softwareindustrie, sind Argumente, die das verständlich machen. Vor allem US-Riesen wie Amazon, Google, Microsoft und Apple kämpfen um die Dominanz in diesem Markt. Diese Unternehmen haben den Plattformgedanken, die Ökonomie des Teilens, die Geschäftsmöglichkeiten von Datenverfügbarkeit und Big Data schon früh erkannt.

Sie alle haben unsere Datenspuren aufgezeichnet. Wer hat in der westlichen Welt mehr biometrische Daten als diese Internetgiganten, mit all ihren Nutzern, die Ihren wie meinen Zugang mit Daumenabdruck und Stimme verifizieren? Diese Daten sind für unsere Privatsphäre entscheidend. Solange die USA das europäische Grundrecht auf die privaten Daten seiner Bürger und Unternehmen akzeptieren und respektieren, ist die Datendominanz der US Unternehmen lediglich eine marktwirtschaftliche Herausforderung, für Europa und seine Unternehmen. Wenn die USA aber die europäischen Datenrechte nicht akzeptieren und keine reziproke Gesetzgebung zulassen, haben wir Europäer und unsere Unternehmen ungleich lange Spieße.

Die Schaffung von Rahmenbedingungen zur Datennutzung, heute Rohstoff für die Geschäftsmodelle der Unternehmen, ist eine politische Aufgabe:

Die Daten europäischer Bürger und Unternehmen dürfen nur gemäß den europäischen Datenschutzregularien (Datenschutzgrundverordnung der EU ab Mai 2018) genutzt werden. Überall auf der Welt. Die Aufgabe der Politik ist es, nicht nur für europäische Unternehmen Datenschutzrichtlinien mit hohen Strafandrohungen einzuführen.

Gleichzeitig ist auch sicherzustellen, dass diese Richtlinien auch von anderen Staaten und deren Unternehmen eingehalten werden. Sonst drohen Wettbewerbsnachteile: Unsere Produktionsdaten und Marktdaten gehen über die EU-Grenzen, werden weltweit vernetzt, in Algorithmen verarbeitet und stehen allen zur Verfügung außer den europäischen Unternehmen. Europäische Artificial Intelligence Applikationen verlieren zunehmend an Wettbewerbsfähigkeit (weil weniger Daten) und wir müssen die in Algorithmen verarbeiteten Daten für die Robotersteuerung, für Marketingkampagnen etc. teuer zurückkaufen.

Ein zweites Feld, bei dem die Politik gefordert ist, liegt in der Cyber-Security. Sacheigentum ist rechtlich stark geschützt, es gibt sichtbare Präsenz der Polizei zum Schutz von Eigentum. Bei Daten wird jedoch nicht von Dieben sondern von Hackern gesprochen. Der Diebstahl von Daten scheint ein Kavaliersdelikt zu sein. Ein Kavaliersdelikt das, wenn man den gegenseitigen Beschuldigungen Glauben schenkt, von Staaten gestützt oder mindestens geduldet wird!

Solange das Dateneigentum materiell und juristisch nicht in den Rang des Sacheigentums gehoben wird, brauchen wir über Datenschutz gar nicht zu sprechen. 72% der österreichischen Unternehmen berichteten 2017, dass sie bereits das Ziel von Cyber Attacken wurden. Es ist die moderne Form der Industriespionage, die sich heute nicht nur auf Technologien, sondern auch auf Prozess- und Kundendaten bezieht. Aber wo ist hier die Polizei? Wo sind die Fahndungserfolge? Es scheint als müssten sich wirklich die Unternehmen auf mittelalterliche Weise selbst schützen?

Datennutzung und Datenschutz sind auch eine Wettbewerbsfrage.

Mit welchen Technologien können wir den Datenschutz und die Datennutzung sicherstellen? Warum sind andere Nationen technologisch so weit vorne, dass wir das Gefühl haben, nicht einmal gleich lange Spieße

beim Datenschutz und bei der geschäftlichen Nutzung unserer Daten zu besitzen?

Wir fragen uns, inwieweit der Wettbewerb über das Web eine globale oder eine regionale Angelegenheit ist. In der westlichen Welt diskutieren wir über Netzneutralität, also die Frage, ob in Zukunft beliebige Gebühren für bessere Datenverbindungen verlangt werden können.

Die wichtigere Frage scheint allerdings zu sein, ob der freie Zugang zum Web nur in einigen Ländern gewährt und in anderen national eingeschränkt wird. Für Europäer ist ein selektives Verbot von Netzwerkdiensten undenkbar. In Russland, China und anderen Staaten ist das normal. Google, Twitter, Facebook etc. werden entweder nicht oder nur nach vorheriger Filterung von Nachrichten oder Suchergebnissen zugelassen. Das Web ist damit weder global noch neutral. Manche Länder machen Netzinformationen für alle zugänglich, andere nehmen und geben Informationen nur selektiv. Sie haben, so wie bei den Protesten im Iran das Internet „fest im Griff".

Das kann politisch motiviert sein, hat aber in vielen Fällen auch den geschäftlichen Hintergrund, die eigenen Unternehmen oder die eigenen Daten zu schützen. Aus diesem Grund finden sich die großen Wettbewerber der amerikanischen Internet Riesen vor allem in China. Was wäre passiert, wenn Google, Facebook und Co. freien Zugang zum chinesischen Markt gehabt hätten, so wie in Europa? Die einseitige Öffnung, der einseitige Zugang zum Web schadet denen, die sich dem freien Zugang und der beschränkten Nutzung von Daten verpflichtet haben: unseren europäischen Unternehmen.

Entsprechend stellt sich die Frage, wie wir unsere Daten gemäß den europäischen Regeln schützen können. Hier dürfte der Zahlungsverkehr eine wichtige Rolle spielen: Je mehr Finanzdaten von Kunden und Unternehmen über außereuropäische Anbieter abgewickelt werden, desto weniger weiß Europa von sich selbst. Nicht nur Swift, Paypal und die Kreditkartenindustrie (die Europäer haben beispielsweise 2015 ihre Anteile an Visa verkauft!) haben außerhalb Europas ihren Sitz, neue Konkurrenten scheinen einmal mehr besagte Internetriesen zu werden (alle haben europäische Banklizenzen erworben und sind teilweise bereits aktiv wie beispielsweise Apple Pay).

Um unsere europäischen Finanzdaten und -informationen gemäß unseren Datenschutzprinzipien in Europa halten zu können, scheint ein einheitliches und überlegenes europäisches Zahlungsverkehrssystem elementar. Wiederum scheint es so, dass Europa zuerst der ganzen Welt die Selbstbedienung im europäischen Datenhaushalt anbietet (siehe PSD2 Richtlinie) und nicht parallel Reziprozität beim Datenschutz einfordert. Allerdings wird versucht, durch ein überlegenes innereuropäisches Zahlungsverkehrssystem, das auf SEPA und – neu– auf Instant Payment aufbaut, den europäischen Zahlungsverkehr zu forcieren. Der Motor dieser Entwicklung ist die EZB.

Gleich lange Spieße bei Datennutzung und –sicherheit sind für Europas Zukunft fundamental

Wenn es Europa nicht gelingt, bei Datennutzung und Datenschutz globale Wettbewerbsgleichheit herzustellen, werden unsere Unternehmen zurückfallen: Bei der Finanzierung (wer hat die Daten zur Bonitätsprüfung?), bei Marketing und Verkauf (wer kennt in Zukunft die Kunden und das Kundenverhalten?), bei der für Europa so wichtigen Automatisierung und Roboterisierung (Wer verfügt über Big Data zur ständigen (Weiter-) Entwicklung von Artificial Intelligence?) und beim Zugang zu fremden Märkten (wer bekommt in Zukunft ein China Visum nach einem kritischen China-Kommentar im Web?).

Die Digitalisierung fordert unsere Politik, vor allem die Politiker der EU. Sie fordert uns alle – mit spannenden Herausforderungen für alle, die Lust haben, sie anzunehmen!!

Wir wünschen Ihnen ein erfolgreiches 2018

Dr. Hannes Enthofer Patrick Haas
Partner Finance Trainer

Luxembourg, 8.1.2018