Christoph Wegener

Was schafft eigentlich Vertrauenswürdigkeit?

Bereits vor etlichen Jahren wurde das papierlose Büro als die Lösung vieler Probleme proklamiert. Bis heute aber halten sich staubige Aktenschränke und Kopierer und Drucker werden ausgiebiger genutzt als je zuvor.

Woran liegt das eigentlich? Neben der tief verwurzelten Gewohnheit der Überschaubarkeit von papiergebundenen Büroabläufen ist ein weiterer Grund sicherlich ein gesundes Misstrauen gegenüber den Schwachstellen der elektronischen Welt und dem Zweck und der Wirksamkeit entsprechender rechtlicher Regelungen. Diese führen dazu, dass eben doch noch immer Papierdokumente produziert und archiviert werden.

Medienbrüche überall

Statt die Kommunikation zu vereinfachen, hat die fortschreitende Verbreitung der elektronischen Kommunikation so dazu geführt, dass Unternehmen, Behörden und auch die Bürger häufig Medienbrüche akzeptieren müssen. Das verkompliziert die Vorgänge, verursacht zusätzliche Kosten und steigert zudem auch die Möglichkeiten von Kommunikationsfehlern. Was liegt also näher, als zu versuchen, mit entsprechenden technischen und rechtlichen Strukturen bestehende Hürden abzubauen.

Von Analog zu Digital

Projekte wie De-Mail und der eID-Funktion des neuen Personalausweises sollen dazu beitragen, die fehlende Verbindlichkeit im heutigen Internet zu mildern und so mehr Vertrauen in die elektronische Kommunikation schaffen.

Notwendigerweise führen diese Projekte aber zu komplexen Infrastrukturen und neuen Diensten, die ihrerseits Vertrauenswürdigkeit einfordern müssen.

Die Kehrseite der Medaille sind also noch mehr dienstspezifische Daten in elektronischer Form und damit ein weiter steigendes Missbrauchspotenzial. Denn liegen Daten erst einmal in elektronischer Form vor, lassen sie sich in vielfältiger Art und Weise verknüpfen, neu auswerten und somit ggf. auch entgegen dem eigentlichen Verwendungszweck, der der Datenerhebung zugrunde lag, gebrauchen und

damit entgegen den ehemaligen Interessen der Betroffenen missbrauchen.

Ohne Zweifel benötigen wir also auch neue Mechanismen, die mit technischen Maßnahmen den Missbrauch von Daten erheblich erschweren oder aber zumindest durch rechtliche Regelungen entsprechende Kontrollen und auch Strafen einführen. Letztere müssen aber zumindest so hoch angesetzt sein, dass die Vorteile, die die verarbeitende Stelle aus einem Missbrauch ziehen kann, deutlich übertroffen werden. Strafgelder mit „Portokassenniveau“ nützen nichts.

Technische Kontrollen

Technische Schutzmaßnahmen sollten dabei aber immer so einfach wie möglich umgesetzt werden, sonst verpufft ihre Wirkung: Entweder diejenigen, die die Kontrollen umsetzen müssen, verzweifeln bei der Umsetzung oder weigern sich (aus Kostengründen) schlicht, die Anforderungen zu erfüllen. Oder aber die Prozesse bergen aufgrund ihrer hohen Komplexität von Grund auf ein enormes Fehlerpotential. Wenn etwa anstelle einer Partei im Rahmen eines aufwendigen Prozesses nun gleich mehreren Parteien vertraut werden muss, hat der Betroffene nicht viel gewonnen.

Vertrauen ist gut, Kontrolle ist besser

Muss man dem Staat eigentlich besonders kritisch gegenüber treten? Häufig wird argumentiert, dass jeder seine Daten an Google, Amazon, Facebook und viele weitere „Datensammler“ weitergibt, ohne auch nur mit der Wimper zu zucken. Der Staat aber werde zu Unrecht verteufelt, wenn er große IT-Projekte umsetzt, die auch mit umfangreicher Datenspeicherung einhergehen, beispielsweise im Falle von ELENA.

Andererseits verwalten die Behörden die Gesellschaft und benötigen dazu Informationen. Es gibt also entsprechend vielfältige Datensammlungen (unter anderem bei Melde- und Finanzämtern sowie der Rentenversicherung), die vollständig, aktuell und richtig sein müssen. Entscheidend ist dabei, dass die Daten nicht zum Nachteil der Betroffenen verknüpft werden dürfen.

Ein solcher Zustand lässt sich in einer demokratischen Gesellschaft vertrauenswürdig aufrecht erhalten. In totalitären

Regimes aber könnten von entsprechenden Datenauswertungen Gefahren für das Ansehen von Personen und für Leib und Leben ausgehen – wie zahlreiche Beispiele leider immer noch zeigen.

Transparenz ist oberstes Gebot

Wir brauchen also bei der Einführung neuer Verfahren eine hohe Transparenz und auch eine Kontrolle durch unabhängige Stellen. Hieraus ergibt sich aber eine zwiespältige Situation: Auf der einen Seite wird nach dem Staat als unabhängigem Kontrolleur bzw. Zertifizierer gerufen. Dem Staat als Betreiber von Infrastrukturen steht man auf der anderen Seite aber grundsätzlich misstrauisch gegenüber.

Fraglich ist auch, ob aber nicht gerade durch immer mehr Regelungen die Prozesse, die durch entsprechenden Wettbewerb, etwa bei Haftungsregelungen, zu einer Verbesserung führen, im Keim erstickt werden. Eine Regulierung ist zudem immer auch eine Form von Bevormundung, entscheidet doch nun durch die Anforderungen zur Zertifizierung indirekt der Staat und nicht mehr der Betroffene, wem etwaige persönliche Daten anvertraut werden können.

Datenschutz: Heute und morgen

Offen bleibt in jedem Fall, ob der heutige Datenschutz das richtige Mittel ist, den (zukünftigen) Anforderungen einer modernen Online-Welt gerecht zu werden. Kontrolle im Sinne von Evaluierung und Zertifizierung sind wohl nicht immer der Königsweg zu einem besseren Datenschutz, denn schlussendlich müssen die Betroffenen doch noch selbst frei entscheiden können, wem sie wann welche ihrer Daten geben wollen.

SchülerVZ, StudiVZ und Co. gehören mittlerweile zu unserem Alltag und auch wenn uns das nicht gefällt, unsere Kinder und Enkel werden mit dabei sein. In diesem Zusammenhang sollte Kontrolle daher eher als verantwortungsvoller Umgang verstanden werden, der vor allem Kindern und Jugendlichen beigebracht werden muss. Und da sind wir alle gefragt, denn jeder Einzelne und nicht der Staat kann und muss hier zu einer Verbesserung des Datenschutzniveaus beitragen!