SocietyByte

BFH-Magazin für die Humane Digitale Transformation

Wenn Behörden ausländische Cloud-Anbieter für die Datenspeicherung nutzen

Von Jonas Bärtschi (BFH Wirtschaft) | 0 Kommentare

Die digitale Souveränität ist eines von drei jährlichen Fokusthemen der «Strategie Digitale Schweiz». Es geht um die Frage, wie sich Abhängigkeiten in der digitalen Welt reduzieren lassen. Ein konkreter Anwendungsfall ist die Behörden-Cloud: Darf eine schweizerische Verwaltung ihre Daten bei einem ausländischen Cloud-Anbieter speichern? Ja, bilanziert ein Podium mit juristischen Fachleuten – wenngleich zum Schutz der Bürger*innen zusätzliche Massnahmen nötig sind.

«Wenn wir die ganze Geschichte mit Snowden und der NSA nicht gehabt hätten, wären alle etwas weniger aufgeregt», erklärt Esther Zysset an der Podiumsdiskussion zur Stadtzürcher Behördencloud. Die Expertin für öffentliches Recht diskutiert mit Christian Laux das Gutachten, das dessen Anwaltskanzlei für die Stadt Zürich verfasst hat. Es bescheinigt der Stadt Zürich, dass die Auslagerung der Behörden-Cloud auf Server ausländischer Hersteller aus juristischer Sicht kein Problem darstellt. Das Podium ist eine gemeinsame Veranstaltung der Berner Fachhochschule und der Swiss Data Alliance, einem unabhängigen Think Tank für konstruktive Datenpolitik [https://www.swissdataalliance.ch/] . Rika Koch vom Institut Public Sector Transformation der BFH [https://www.bfh.ch/de/forschung/forschungsbereiche/public-sector-transformation/] moderiert das Gespräch.

Die drei Fachpersonen sind sich einig: Wenn eine Behörde mit ihren Daten in die Cloud geht, trägt sie eine Verantwortung – sie muss wissen, was technisch passiert, aber auch, welche vertraglichen und rechtlichen Rahmenbedingungen existieren. Deshalb brauche es auch kein zusätzliches Gesetz, argumentiert Christian Laux: «Die politische Diskussion darf sich nicht hinter den rechtlichen Fragen verstecken. Denn die Rechtmässigkeit und Verhältnismässigkeit einer Cloud-Lösung für Behördendaten ist in erster Linie eine Frage der korrekten, sorgfältigen Umsetzung.»

Tatsächlich sei die Aufschlüsselung der Verantwortung nach politischem Willen, technischen Rahmenbedingungen und konkreten Anforderungen an eine jeweilige Organisationseinheit sinnvoll, bescheinigt Esther Zysset. «Schwierig sind jedoch die Aspekte, die mit dem Auslandsbezug zu tun haben.» Es gäbe keinen adäquaten Rechtsschutz für Bürgerinnen und Bürger, wenn beispielsweise eine ausländische Behörde die Herausgabe von Daten über eine Person forderten. Das sieht auch Christian Laux so: «Man kann nicht mehr zu 100% garantieren, dass bei einem Gerichtverfahren im Ausland kein Zugriff auf die Daten geschieht. Hier gibt es auf eidgenössischer Ebene Handlungsbedarf.»

Weniger Bedenken haben die Fachleute jedoch im Hinblick auf den Zugriff durch Geheimdienste, etwa unter dem amerikanischen CLOUD Act. «Sobald amerikanische Behörden die Herausgabe von Daten verlangen, wird bereits der Cloud-Provider informieren, dass es sich um die Daten einer Behörde handelt.» Die amerikanische Behörde würde dann die Stadt Zürich kontaktieren – und diese könnte den Fall in die Schweiz bringen und nach Schweizer Gerichtstand behandeln lassen.

Einzig aus staatsrechtlicher Sicht gehe ihr das Gutachten in einem Punkt zu weit, meint Esther Zysset: «Das Gutachten beschreibt, wie eine Behörde den Gang in die Cloud genehmigen und sich so de facto über das Amtsgeheimnis hinwegsetzen kann. Das bedeutet letztlich, dass ein Exekutivbeschluss höheres Gewicht hat als das durch die Legislative verabschiedete Gesetz.» Allerdings sei dies nur problematisch, wenn die Genehmigungen sehr pauschal geschähen statt von Fall zu Fall, räumt sie ein.

Die Aufnahme der Podiumsdiskussion ist hier zu finden [http://www.swissdataalliance.ch/cloud] .

Fokus Datensouveränität

Als Teilaspekt der digitalen Souveränität formuliert die Datensouveränität, was im Zusammenhang mit Daten zu tun ist, damit ein Staat souverän handeln kann. Dabei stehen drei Aspekte im Fokus:

1. Die Kompetenzabgrenzung gegenüber anderen Staaten (z.B. Vorgehen bei einer Strafverfolgung im Ausland)
2. Die Gestaltungshoheit im Hinblick auf die eigenen Daten (z.B. kommerzieller bestimmter datenbezogener Transaktionen)
3. Die Abwehrfähigkeit gegenüber Angriffen von aussen (z.B. Schutz vor Spionage)

Ein neu erwachtes Interesse am Souveränitätsbegriff zeigt sich auch in der Vielzahl von Interessensgruppen, die eine jeweilige Neuinterpretation des Begriffs und damit des Staatsverständnisses vorantreiben. Um einen konstruktiven Diskurs zu ermöglichen, hat die Swiss Data Alliance ein Begriffspapier publiziert [http://swissdataalliance.ch/datensouveränität] , das die Ankerpunkte der Datensouveränität zusammenfasst.

Die Swiss Data Alliance [https://www.swissdataalliance.ch/] engagiert sich für eine konstruktive Datenpolitik an der Schnittstelle von Forschung, Wirtschaft und Zivilgesellschaft.

AUTHOR: JONAS BÄRTSCHI

Jonas Bärtschi ist wissenschaftlicher Mitarbeiter am Institut Public Sector Transformation. Er ist Geschäftsführer der Swiss Data Alliance.

Posts from Jonas Bärtschi | Website

Create PDF

Ähnliche Beiträge

Datenkolonialismus und die Rolle des öffentlichen Sektors
Sprachmodelle und Natural Language Processing - ein Rückblick auf die Transform-Konferenz 2023
Was ein zeitgemässes Identitätsmanagement-System erfüllen soll
«Wir sind alle mit dem Phänomen Datenkolonialismus verbunden»

0

COMMENTS