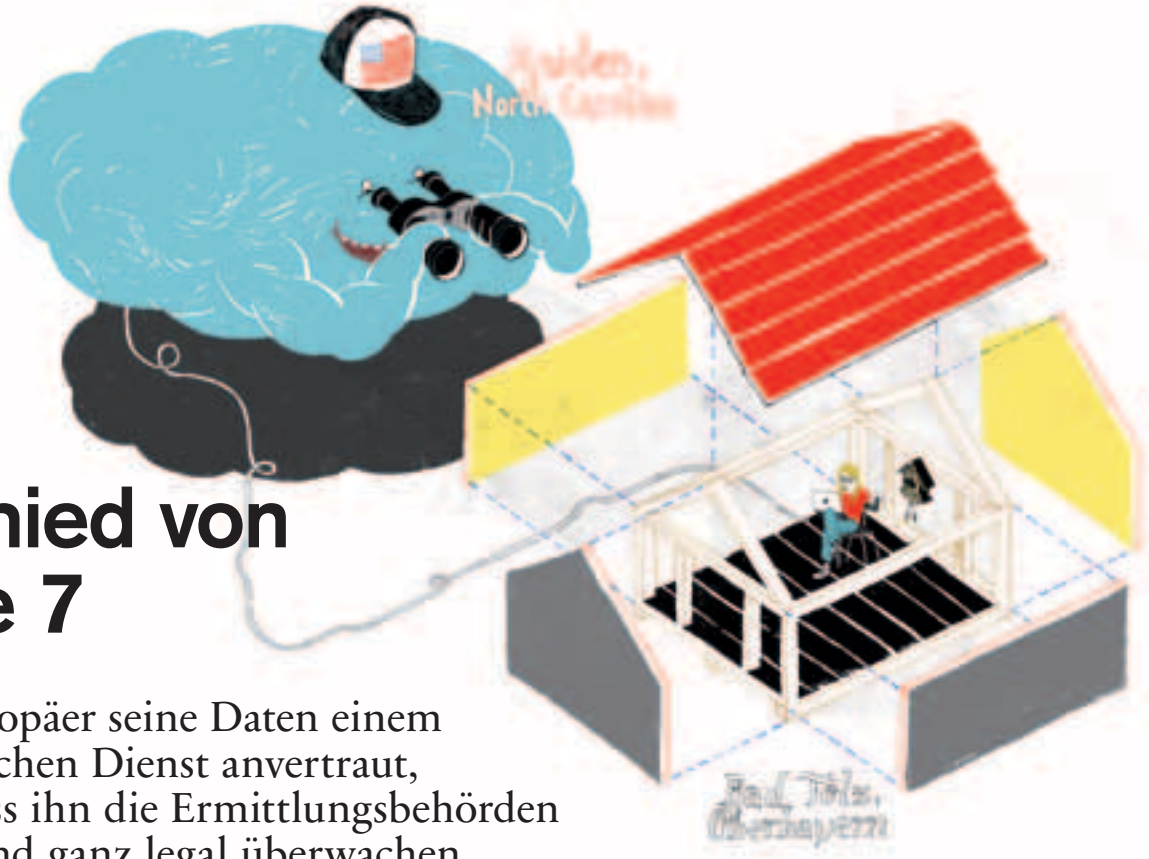

Abschied von Wolke 7

Wer als Europäer seine Daten einem amerikanischen Dienst anvertraut, riskiert, dass ihn die Ermittlungsbehörden heimlich und ganz legal überwachen

Text: Arne Semsrott

→ „Ich fühle mich, als ob ich im kommunistischen Russland leben würde, nicht in den USA“, sagte der ehemalige US-Soldat Abe Marshal der Presse, als ihm das FBI mitteilte, er stehe auf ihrer „No-Fly List“. Damit darf er im gesamten Land kein Flugzeug mehr besteigen. Der Grund für das Verbot? Marshal hatte sich bei einem Imam – also einem islamischen Prediger – per E-Mail über islamische Kindererziehung informiert. Das FBI hatte den Briefwechsel abgefangen und als gefährlich eingestuft.

Die amerikanischen Geheimdienste investieren seit einigen Jahren riesige Summen, um die Kommunikation im Internet effektiver abhören zu können. Dabei geraten durch die Nutzung von sogenannten Cloud-Computing-Diensten neben Amerikanern auch Europäer ins Visier von US-amerikanischen Ermittlern, wenn ihre Daten auf amerikanischen Servern liegen.

Immer mehr Privatleute und Unternehmen speichern ihre Daten in einer Cloud, zu der sie von jedem Rechner der Erde übers Internet Zugang haben. Das ist nicht nur praktisch, viele Firmen versprechen sich davon mehr Sicherheit vor Systemausfällen, niedrigere Kosten und flexiblere Arbeitsbedingungen. Anstatt die Daten auf der eigenen Festplatte zu speichern, schieben viele Internetnutzer Programme, Arbeitsdokumente und Musik in die Cloud – allerdings sind sie dort nicht nur für den Urheber abrufbar.

Denn liegen die Daten erst einmal in der Cloud, die in Wahrheit natürlich ein Server ist, ist es schwierig festzustellen, ob sie noch in Deutschland oder in den USA gespeichert sind und welchen Gesetzen sie damit unterliegen. Die Datenschutzbestimmungen im alten Europa unterscheiden sich erheblich von denen in den USA.

Ist sowohl der Anbieter der Cloud als auch der Nutzer in der EU beheimatet, gilt der europäische Datenschutz. Genauso, wenn amerikanische Cloud-Provider reine EU/EWR-Clouds anbieten und vertraglich festgelegt ist, dass die Daten in bestimmten Rechenzentren verarbeitet werden und den europäischen Wirtschaftsraum nicht verlassen dürfen. Das bedeutet, dass Daten gegenüber Zugriffen von außen geschützt und nach dem Willen der EU-Kommission bald auch auf Verlangen der Nutzer gelöscht werden müssen.

Bei Anbietern wie Google, Microsoft, Dropbox oder Apple (iCloud) ist das allerdings anders, da sich ihre Server womöglich auf US-Territorium befinden. Wie eine Studie im Auftrag des Europäischen Parlaments ergab, haben die amerikanischen Bundesbehörden dort seit Einführung des Patriot Act umfangreiche Befugnisse. Als Antwort auf die Terroranschläge vom 11. September 2001 sicherte die US-Regierung dem FBI und anderen Geheimdiensten gesetzlich die Möglichkeit zu, Telefone unbemerkt abzuhören, Universitäten und Bibliotheken zu überwachen und E-Mails auszuspionieren. Bei einem Tatverdacht haben sie auch ohne Gerichtsbeschluss das Recht, Daten von Providern anzufordern. Was ein Tatverdacht ist, entscheiden die Behörden selbst.

Wer dann ins Visier der amerikanischen Terrorfahnder gerät, ist nur sehr schwer nachzuvollziehen. Noch schwieriger ist es, sich gegen mögliche Folgen zu wehren.

So könnte unter Umständen schon der Austausch von Cloud-Daten mit islamischen Gelehrten genügen, damit das FBI den Nutzer auf eine „No-Fly List“ setzt. Abe Marshals Name steht trotz massiven Protests noch immer auf der Liste. ←