1. Wem gehören meine Daten?

Eigentum bleibt Eigentum, auch wenn die Besitzverhältnisse undurchsichtig sind oder sogar wechseln. Meiner Meinung nach gilt das auch und gerade besonders für die Daten, die sich über mich anhäufen – Daten, die sich aus meiner Online-Aktivität und meinem Umgang mit elektronischen Medien ergeben. Diese Daten sind allerdings nicht ausschließlich in meinem Besitz. Oftmals sind sie sogar gar nicht in meinem Besitz, weil ich Dienste nutze, die ebenjene Daten für sich beanspruchen und die dahintersteckenden Firmen sie weiterverkaufen. Dabei verkaufen sie **meine** Daten; **mein** Eigentum.
Die Frage ist nur, ob sie noch länger mein Eigentum sind, wenn ich meine Daten im Rahmen der Benutzung der Dienste erschaffe – in meinem Besitz sind sie ohnehin nicht (und wenn, dann in einem solchen Zustand, dass sie die Firmen nicht weiterverkaufen können). Außerdem habe ich den Firmen, wenn ich ihre Dienste benutze, sogar erlaubt, dass sie meine Daten verwenden dürfen.
Aber die Daten sind nur etwas wert, wenn sie eindeutig **zu** mir gehören, denn sonst ließen sie sich nicht verkaufen. Und wenn etwas nur Bedeutung hat, wenn und weil es **zu** mir gehört, dann gehört es auch mir – oder sollte vielmehr mir gehören.

2. Wie schütze ich meine und andere Daten?

Meine Daten sind unmöglich zu schützen, wenn sie durch und für die Dienste entstehen, die ich benutze. Die Firmen hinter diesen Diensten sammeln sie zwangsläufig und nutzen sie dementsprechend. Manchmal, um mir selbst Annehmlichkeiten und Funktionalität zu gewährleisten, hauptsächlich jedoch (insbesondere bei Diensten, die mich kein Geld kosten), damit die Firmen sich selbst finanzieren können. Der wirksamste Schutz dem gegenüber ist vollständiger Verzicht auf die entsprechenden Dienste oder die Inkaufnahme von Einschränkungen.
Wenn man dennoch Daten preisgibt, geschieht dies immer aus einer Verantwortung heraus. Andere Daten, die nicht mir gehören, darf ich nicht anders behandeln, wie ich möchte, dass meine eigenen Daten behandelt werden. Dasselbe sollte auch für deren Schutz gelten.
Datenschutz fängt mit einer eigenen Sensibilität für datenschutztechnische Risiken an. Dazu gehört, sich über die Risiken bewusst zu sein und Maßnahmen zu ergreifen. Zum Beispiel, die Rechte benutzter Dienste einzuschränken oder bestimmte Features gar nicht erst zu nutzen.
Datenschutz hört aber nicht dort auf, wo ich die Sammelaktivitäten bestimmter Firmen unterbinde. Dazu gehört auch ein sorgsamer Umgang im Netz, um nicht Opfer von Cyberkriminalität zu werden. Datenklau durch Viren, Würmer, Trojaner – und wie die Schadprogramme alle heißen – gilt es zu unterbinden, indem man Vorkehrungen trifft; zum Beispiel einen Virenschutz eines seriösen Anbieters zu installieren und Sicherheitsvorkehrungen zu treffen, wie beispielsweise eine Firewall zu errichten. Auch Maßnehmen zu ergreifen gegen Visual Hacking oder den Schutz etwaiger geklauter physischer Datenträger ist sinnvoll.