Modell und Wirklichkeit

Jede technische oder rechtliche Betrachtung von Fragen des Datenschutzes oder der Informationssicherheit fußt auf einer ganz bestimmten Sicht der Welt, einem Bild, das wir uns von der Wirklichkeit machen, oder, wie der Informatiker sagen würde, einer Modellierung. Jede solche Modellierung ist – unvermeidlich und gewollt – eine Vereinfachung; sie ist nie vollständig und daher auch nie „richtig“, wenn auch nicht gänzlich falsch. Sie fokussiert auf einen bestimmten Aspekt oder eine spezielle Eigenschaft der Wirklichkeit. Und sie dient dazu, die Komplexität zu reduzieren, um uns einen möglichst einheitlichen Umgang mit der Realität zu ermöglichen.

Diese Modellbildung hat allerdings Grenzen, vor allem im Datenschutz. Wenn wir uns aus der rein technischen oder der rein rechtlichen Perspektive mit Datenschutzfragen befassen, blenden wir jeweils große Bereiche aus. So können wir beispielsweise rechtlich die Vertraulichkeit von Daten bei einer digitalen Übermittlung nicht sicherstellen – das ist eine technisch zu lösende Aufgabe, die sich in Details entscheidet (Verschlüsselungsverfahren, Schlüssellängen, fehlerfreie Implementierung, Schlüsselmanagement etc.). Allerdings können wir wiederum technisch nicht sicherstellen, dass personenbezogene Daten auch tatsächlich verschlüsselt werden – das erreichen wir wiederum (indirekt) durch rechtliche Maßnahmen wie die Verpflichtung zu geeigneten Schulungen und die Zuweisung von Verantwortung für die Umsetzung dieser Verpflichtung. Erst in der Kombination beider Perspektiven, der rechtlichen und der technischen, wird Datenschutz damit tatsächlich wirksam (siehe z. B. *Ronald Petrlc* zur Verbreitung von HTTPS in diesem Heft).

Zumindest theoretisch. Denn in der Praxis haben wir es mit Menschen und „Schnittstellen“ zur Technik zu tun – und da sind unsere Modelle manchmal ebenfalls unzureichend. Denn eine hervorragende technische Lösung kann wiederum am Verständnis der Nutzer (oder auch anders herum das Verständnis der Nutzer an der komplexen oder unverständlichen technischen Lösung) scheitern. So ist es interessant zu sehen, wie beispielsweise die von Technikern und Datenschützern begrüßte Ende-zu-Ende-Verschlüsselung des Messenger-Dienstes WhatsApp von Nutzern wahrgenommen wird (siehe den Beitrag von *Nina Gerber*, *Verena Zimmermann*, *Birgit Henhagl*, *Sinem Emeröz*, *Melanie Volkamer* und *Tobias Hilt* in diesem Heft).

Und gelegentlich ändert sich die Welt, weil neue Techniken sich verbreiten (Internet, Smartphones, Cloud-Dienste, Soziale Netzwerke, Connected Cars) – und auf einmal passt unser technisches oder rechtliches Modell nicht mehr. Es entstehen andere, neue Bedrohungen (Cloud-Dienste, Connected Cars), oder die Verantwortung für die verarbeiteten Daten ist nicht mehr so eindeutig zuzuordnen (Facebook). Rechtlich können wir das eine oder andere über Gerichtsurteile und „herrschende Meinungen“ korrigieren, aber manchmal ist das Modell überfordert. Ein Beispiel dafür sind die so genannten Fitness Tracker; ihre datenschutzrechtliche Bewertung beleuchten *Charlotte Husemann*, *Fabian Pittroff* und *Andreas D. Schulz* in diesem Heft. Ein weiteres kommt aus dem Gebäudemanagement: Wer den Energieverbrauch in Bürogebäuden (für Heizung, Klimatisierung, Gerätebetrieb) wirksam senken möchte, wird irgendwann über eine dynamische Anpassung an das Nutzerverhalten nachdenken – mit allen damit zusammenhängenden datenschutzrechtlichen Fragen, näher untersucht im Beitrag von *Anders Berg*, *Steffen Braun* und *Tobias Henzler*.

Wie so oft steckt der Teufel im Detail – Komplexität, Mehrdimensionalität und Volatilität der Realität machen die datenschutzkonforme Gestaltung von Technik zu einer permanenten Herausforderung. Das wollen wir in diesem Heft beispielhaft zeigen.

Dirk Fox