Offene Herausforderungen

Das große, „disruptive" (so würde man es wohl inzwischen bezeichnen) Projekt des 21. Jahrhunderts ist die Digitalisierung. Seine Wurzeln reichen tief ins ausklingende 20. Jahrhundert zurück, aber erst in den letzten 10-15 Jahren nimmt es kräftig Fahrt auf. Kaum noch ein Bereich unserer Gesellschaft, der von der digitalen Verarbeitung von Daten verschont bliebe. Mehr noch: Durch die wachsende Verbreitung von Anwendungen („Apps") werden ständig weitere Lebensbereiche zu unterschiedlichsten Zwecken digital vermessen – insbesondere auch solche, die in der Vergangenheit einer Erfassung nicht zugänglich waren, wie Bewegungsprofile (GPS-Daten), Gesundheitsdaten (Fitness-Tracker, Herzfrequenz) oder das gesprochene Wort (Spracherkennungs- und Steuerungssysteme).

War in den frühen Anfängen der Digitalisierung das Bundesdatenschutzgesetz den technischen Möglichkeiten noch weit voraus – das Jahr des Volkszählungsurteils war das Jahr zwei des IBM-PC – hat das Datenschutzrecht inzwischen Mühe, der rasanten Entwicklung der technischen Möglichkeiten angemessene Rahmenbedingungen und Grenzen zu setzen. Während die überbordenden Datenschutz-Einwilligungen (Wissen Sie, wie viele Einwilligungen Sie bereits in diesem noch jungen Jahr erteilt haben? Und haben Sie zu jeder die Datenschutzerklärung gelesen?) zu Generallegitimationen für jede noch so weit gehende Verarbeitung verkommen, entstehen zugleich immer riskantere Datensammlungen. Eine ganz besondere Herausforderung stellen in diesem Zusammenhang humangenetische Daten dar, die in der Biomedizin eine immer wichtigere Rolle spielen, wie *Hamacher*, *Katzenbeisser*, *Kussel* und *Stammler* in ihrem Beitrag zeigen.

Auch die praktische Anwendung des geltenden Datenschutzrechts auf konkrete Datenverarbeitungen ist nicht immer so eindeutig, wie man sich das von einer Regulierung eigentlich erhofft. So ist die Datenschutz-Grundverordnung noch immer für zahlreiche offene Fragen gut. In diesem Heft gehen *Hessel* und *Potel* der Frage nach, ob auch solche Datenschutzvorfälle meldepflichtig sind, die verschlüsselte Daten betreffen. Von *Weik* wird die in der Praxis durchaus relevante Frage diskutiert, ob die Übersendung einer Kopie der verarbeiteten Daten als integraler Bestandteil des Auskunftsrechts nach Art. 15 DSGVO oder als unabhängiger Anspruch des Betroffenen zu verstehen ist.

Praktische Herausforderungen stellen sich auch beim Löschen (Art. 17 DSGVO) und bei der Umsetzung des Prinzips Data Protection by Design and by Default (Art. 25 DSGVO). Wie das funktionieren kann, stellen die Erfahrungsberichte von *Koch*, *Weide* und *Pawils* zur Anwendung des Standard-Datenschutzmodells in der Telematikinfrastruktur des Gesundheitswesens und von *Knuchel* und *Ebert* zum Löschen in CRM-Systemen vor.

Zwei wichtige Elemente eines wirksamen Schutzes personenbezogener und anderer schützenswerter Daten sind die Sensibilisierung der Mitarbeiter für konkrete Gefährdungen und die systematische Untersuchung von IT-Systemen auf existierende Sicherheitslücken. *Hilt* und *Volkamer* untersuchten dafür exemplarisch die Eignung wichtiger Informationsangebote im Internet zu Phishing-Angriffen. Und *Wagner* beleuchtet die nach wie vor unbefriedigende Rechtslage von Forschern bei der Suche nach Schwachstellen.

Die Beiträge zeigen, dass es keineswegs der schiere Umfang der Verarbeitung personenbezogener Daten allein ist, der den Datenschutz vor praktische Herausforderungen stellt. Auch die sich ständig ausweitende Qualität der verarbeiteten Daten und zahleiche konkrete Umsetzungsfragen zwingen dem Datenschutz eine Dynamik auf, die im Vergleich mit anderen Rechtsgebieten zumindest ungewöhnlich ist. Und es ist zu befürchten, dass diese Dynamik in den kommenden Jahren nicht nachlassen wird – ganz im Gegenteil.

Dirk Fox