Privatsachen

Der Umgang mit modernen, mobilen und nicht-mobilen (IT-)Geräten, die aus unserem Alltag längst nicht mehr wegzudenken sind, hinterlässt Unmengen an Datenspuren. Vor diesem Hintergrund steht der vorliegenden Schwerpunkt dieser Ausgabe mit dem Titel „Schutz der Privatsphäre?!? – Technische und rechtliche Überlegungen".

Fest steht: Die aktuelle Datenschutzgesetzgebung stammt vorwiegend aus einer Zeit, in der die Verbreitung und auch das Ausmaß der mobilen Kommunikation mit den heutigen Erscheinungsformen nicht vergleichbar war. Da wundert es nicht, dass viele moderne Techniken nicht entsprechend berücksichtigt sind, was zudem bei wirklich strikter Anwendung der rechtlichen Vorgaben zu mancher Überraschung bzgl. der Rechtmäßigkeit moderner IT-Systeme und -Prozesse führen würde. Und so wird der Ruf nach passenden Datenschutzregelungen immer lauter.

Aber liegt das Problem für unser aller Privatsphäre darin, dass es keine bzw. nur unzureichende rechtliche Vorgaben gibt? Fehlt es denn wirklich an technischen Lösungen? Oder ist es nicht vor allem auch eine gesellschaftliche Problematik, die ein völliges Umdenken in Punkto Privatsphäre erforderlich macht? Diesen Fragen gehen die Autoren dieses Schwerpunktheftes nach, zeigen anhand konkreter Beispiele die Problemfelder der Praxis auf und stellen zudem auch mögliche Lösungsansätze vor:

- Der Beitrag **Zukunft von Datenschutz und Privatsphäre in einer mobilen Welt** von Marit Hansen gibt als Appetizer einen Einblick in kommenden Szenarien und zeigt dabei auch auf, was diese aus Sicht des Datenschutzes bedeuten könnten.
- Jürgen Brauckmann geht in seinem Beitrag dann auf die Thematik **Datenschutzüberraschungen durch Authentisierung und Verschlüsselung** ein. Anhand konkreter Beispiele zeigt er auf, welche Informationen die zur kryptographischen Sicherung eingesetzten Mechanismen, wie bspw. Zertifikate und Schlüssel, enthalten.
- Anschließend erläutern Martin Rost und Christian Krause die Thematik **Relativer Vertraulichkeitsschutz mit TrueCrypt** und zeigen dabei auf, unter welchen Annahmen sich mit dieser -mittlerweile nicht mehr gepflegten- Verschlüsselungssoftware noch ausreichend Schutz erzielen lässt.
- **Technische Prüfung der Datenflüsse beim Smart-TV von Seiten der Aufsichtsbehörden** von Andreas Sachs und Miriam Meder zeigt anhand des Beispiels moderner, an das Internet angebundener TV-Geräte, mit welchen Daten(ab)flüssen der Anwender hier -teilweise völlig uninformiert- konfrontiert ist.
- Alexander Rossnagel und Maxi Nebel weisen in **(Verlorene) Selbstbestimmung im Datenmeer – Privatheit im Zeitalter von Big Data** zu Recht darauf hin, dass moderne und sich fortentwickelnde technische Methoden große Probleme aufwerfen und von aktuellen rechtlichen Vorgaben nur unzureichend berücksichtigt werden.
- Alexander Novotny und Sarah Spiekermann beleuchten dann in ihrem Beitrag **Personenbezogene Daten privatwirtschaftlich nachhaltig nutzen** technische und regulatorische Ansätze und diskutieren, ob und ggf. wie moderne Mechanismen, wie bspw. Big Data, mit den Anforderungen des Datenschutzes Einzelner und der gesamten Gesellschaft in Einklang zu bringen sind.

Ergänzt wird der Schwerpunkt des Heftes diesmal durch zwei Aufsätze:

- Gabriel Schulz zeigt in seinem Beitrag **Informationssicherheit in Kommunen**, welches Mindestsicherheitsniveau der IT-Planungsrat für die Informationssicherheit in der öffentlichen Verwaltung fordert.
- Der Beitrag **On the Security of International Data Exchange Services for E-Governance Systems** von Kim Hartmann und Christoph Steup analysiert, welche Methoden für den grenzüberschreitenden Datenaustausch existieren, und bewertet diese grob in Punkto Datenschutz und Informationssicherheit.

Zusammen mit dem gesamten Herausgeberteam wünsche ich Ihnen als Gastherausgeber eine informative und spannende Lektüre. Wir hoffen, dass auch diese Ausgabe Ihnen, verehrte Leserinnen und Leser, viele Anregungen für Ihren Arbeitsalltag gibt.

Christoph Wegener