

Entwicklung eines Anwendungsszenarios für das Internet of Things im Bereich der privaten Beobachtung.

Patrick Heinker

Die RFID-Technologie (Radio Frequency Identification), als eine der Schlüsseltechnologien des Internet of Things (IoT), ermöglicht die eindeutige, automatisierte und vor allem kontaktlose Erfassung von Objekten, teilweise aus einer Distanz von über einem Kilometer. RFID verbreitet sich gegenwärtig rasant in immer mehr Anwendungsgebieten, besonders in der Automatisierung von Produktionsabläufen und in Lieferketten. Fallende Preise der Systemkomponenten führen dazu, dass diese Technologie immer stärkeren Einzug in unseren Alltag erhält. Bekannte Anwendungen sind hier beispielsweise elektronische Skipässe, Mautsysteme, die elektronische Wegfahrsperre oder auch der neue elektronische Reisepass. Geht es nach den Vorstellungen zahlreicher Befürworter dieser Technologie, sollen künftig sämtliche Alltagsgegenstände mit kleinen Mikrochips versehen werden, um eine weltweit eindeutige elektronische Identifikation von Objekten zu ermöglichen. In Kombination mit dem heutigen Internet könnte so mittelfristig ein „Internet der Dinge“ entstehen, welches gänzlich neue Anwendungen, aber auch Gefahren hervorbringen würde.

Die Tatsache, dass Mikrochips nahezu unsichtbar an Gegenständen angebracht und ohne Sichtkontakt – auch heimlich – ausgelesen werden können, sorgt für starke Bedenken bei Datenschützern und Verbraucherschutzorganisationen. So könnten Person- und Bewegungsprofile erstellt und ausgewertet werden, welche auf unsere Vorlieben, unsere Laster und auch auf unsere sozialen Kontakte schließen ließen. Es ist daher kaum verwunderlich, dass im Zusammenhang mit der RFID-Technologie auch stets das Risiko der totalen Überwachung durch Staat, Unternehmen, neugierige Nachbarn oder auch durch Kriminelle thematisiert wird, welches unserem Grundrecht auf informelle Selbstbestimmung entgegensteht. Gegenstand dieser Arbeit ist daher die zentrale Frage, wie stark der Einsatz der RFID-Technologie künftig zu Beobachtung, Verknüpfung und Auswertung von Konsumentenverhalten sowie der Ausnutzung von privaten Daten führen kann und inwieweit bestehende Datenschutzbestimmungen oder –gesetze vor dieser Ausnutzung schützen.

In der Grobstruktur beschäftigt sich die Arbeit zunächst mit den Grundlagen der RFID-Technologie, deren mögliche zukünftige Entwicklung und deren Potenzial zur Beobachtung von und Informationssammlung über Personen. Ferner werden

wichtige Begriffe aus aktuellen Datenschutzdebatten wie „informelle Privatheit“ und „Schutzmaßnahmen zum Schutz der Privatsphäre“ erläutert. Das dritte Kapitel beschreibt die Szenario-Technik als eine der gängigen Methoden in der wissenschaftlichen Zukunftsforschung. Das vierte Kapitel nutzt diese Technik, um zuerst Einflussbereiche des Internets of Things zu identifizieren, Deskriptoren für diese Einflussbereiche abzuleiten und anschließend mögliche Ausprägungen für diese Deskriptoren aufzuzeigen. Dabei werden bewusst zwei gegensätzliche Ausprägungen vorgestellt, um im anschließenden fünften Kapitel auf Basis dieser unterschiedlichen Ausprägungen zwei Extremszenarien zu beschreiben; eines dieser Szenarien beschreibt dabei eine positive Entwicklung der Deskriptoren im Hinblick auf das Internet der Dinge, das andere hingegen eine Entwicklung der Deskriptoren, die eher hinderlich für das IoT sind. Im sechsten Kapitel werden die Szenarien vor dem Hintergrund aktueller nationaler und europäischer Gesetzgebung durchleuchtet und datenschutzrechtlich analysiert. Dabei zeigt sich, dass die bestehenden Datenschutzgesetze, allen voran das Bundesdatenschutzgesetz (BDSG), die möglichen Überwachungspotenziale im Internet of Things abdecken und die heimliche Überwachung verbieten, jedoch nicht verhindern können.

Letztendlich wird die Frage aufgeworfen, ob es durch Gesetze überhaupt möglich ist, eine Überwachung auf Basis von vernetzten Endgeräten und Verknüpfung mit personenbezogenen Daten zu verhindern. Es wird aber auf verschiedene Grundsätze verwiesen, wie zukünftige Gesetze gestaltet sein müssen, um die zukünftige technische Entwicklung zu berücksichtigen und das Recht auf informationelle Selbstbestimmung zu gewährleisten