Helmut Reimer, Christoph Wegener

Privatsphäre am Scheideweg

Selten klaffen eine fiktive Rechtswirklichkeit und ihr Einfluss auf den täglichen Gebrauch von elektronischen Kommunikations- oder Informationsmedien weiter auseinander: Informationelle Selbstbestimmung und Privatsphäre sind Schlüsselworte für die gesellschaftliche Bewertung von Internet-basierten Diensten und Anwendungen. Beide Begriffe sind nicht scharf definiert, so dass sie meist anhand des Schutzes personenbezogener Daten erläutert werden. Damit werden sie an einen starren datenschutzrechtlichen Rahmen gebunden, dessen Reformbedarf hoch aktuell, aber auch teilweise strittig ist. Betrachtet man das Spektrum der globalen Kommunikationstechnologien, so ist bisher nichts dazu geeignet, Informationen vor dem Ausspähen zu schützen – die Beiträge dieser DuD-Ausgabe illustrieren diesen Sachverhalt vielfältig.

Man muss wohl einräumen, dass die hochdynamischen (und weitgehend unaufhaltsamen) Entwicklungen bei Hardware, Diensten und Anwendungen alle statischen rechtlichen Vorgaben „überschatten“. Sie stehen allen Internet-Nutzern weltweit zur Verfügung und sind milliardenfach verbreitet. Da es auch einen gesellschaftlichen Konsens gibt, dass ihre Nutzung für Bildung und Unterhaltung, Einkauf und Banking sowie Zugang zu Diensten und Kommunikation unverzichtbar sei, ist praktisch jeder Nutzer dazu gezwungen, Bedingungen zu akzeptieren, die die Anbieter festlegen. In der Praxis ist es dabei Tatsache, dass dadurch die nationalen Datenschutzvorschriften (nahezu) unwirksam sind.

Mobile Endgeräte sind (fast) immer im Netz. Als mehr oder weniger offenes „Sensorbündel“ können sie alles verraten, was ihnen an Daten zur Verfügung gestellt wird. Praktisch alle App's greifen darauf zu und bedienen intransparent Interessenten im Netz, informieren dabei sogar den Nutzer über den spezifischen Datenhunger und verlangen dessen Zustimmung. Ein Verzicht auf App's heißt aber praktisch ein Verzicht auf vermeintlich „lebenswichtige“ Anwendungen. Die mobilen Endgeräte bieten darüber hinaus zahlreiche Zugriffsmöglichkeiten von – und auch auf – beliebige Kommunikationspartner.

Cloud und Big Data sind Begleiterscheinungen, die neuerdings mit Anwendungen und Diensten verbunden sind, die der Nutzer nicht souverän verwenden kann. Die dazu gehörenden Infrastrukturen sind intransparent vernetzt, der jeweils unsichere Dienst entscheidet dann über die Widerstandsfähigkeit gegen Zugriffe auf Informationen in der Cloud oder im Big Data-Paket. Immer in Betracht zu ziehen ist außerdem die Speicherung von Meta- bzw. Verbindungsdaten – auch bzw. vor allem durch die „Dienste“ in aller Welt.

Unter diesen Bedingungen ist es wohl richtig festzustellen: Das „Vertrauen“ in die Leistungen des Internets ist heute darauf reduziert, dass hoffentlich diesmal nichts schiefgeht! Mindestens für einen wirksamen Schutz der Privatsphäre sind im Umfeld der allgemeinen Digitalisierung aber neue Ansätze zu prüfen. Auf den ersten Blick erscheint es ein vernünftiges Vorgehen zu sein, die per-se privaten Daten vom größeren Paket der personenbezogenen Daten, die in vielen Zusammenhängen anfallen, konsequent zu trennen.

Aber Privatsphäre – was ist das eigentlich? Geheimnisse, die man nicht verrät, aber dennoch gelegentlich mit vertrauten Personen teilen möchte. Kann das auch elektronisch gut gehen? Vieles spricht dagegen, denn Metadaten verraten die Verbindung, selten gibt es eine „sichere“ Identität, Verschlüsselung wirkt als Angriffsschreiz, gespeicherte Information wirken als Angriffsziel und vieles mehr.

So bleibt eine strikte Trennung in Daten, die man als Geheimnis erhalten möchte (und daher wenn überhaupt nur mit einem sehr engen Kreis von Personen teilt) und solche, die öffentlich werden sollen und dürfen. Dies wäre aber zum einen völlig widersprüchlich zum Einsatz moderner IT-Systeme, deren Anwendungen in vielen Fällen darauf basieren, dass möglichst viele Daten geteilt werden. Zum anderen müsste man auch kritisch hinterfragen, ob und wie man dem Problem begegnen kann, dass auch heute unwichtig erscheinende Daten durch den Einsatz neuer Technologien in Zukunft plötzlich zu neuen Geheimnissen heranreifen. Big Data zeigt hier aktuell eindrucksvoll auf, zu welchen Auswüchsen das führen kann.

Und nicht zuletzt ist auch zu diskutieren, wem ein Geheimnis eigentlich gehört: Der Person, auf die es sich bezieht oder vielmehr demjenigen, der es ermittelt hat? Hier wären bspw. Gesundheitsdaten zu nennen, bei denen auch argumentiert wird, dass ein zu strenger Datenschutz neue Analysemethoden von Massendaten verhindert und damit die Bewertung und Behandlung von Krankheiten erschwert.

Es bleiben viele offene Fragen – die der Einzelne nicht lösen kann und die auch nicht allein durch regulatorische oder technische Ansätze in den Griff zu bekommen sind. Vielmehr sind es Herausforderungen, an denen wir als Gesellschaft unter Berücksichtigung aller Vor- und Nachteile aktiv mit diskutieren und arbeiten müssen: Ob die kommende EU-Datenschutzgrundverordnung dabei tatsächlich das Ende der Fahnenstange ist, bleibt abzuwarten.