Privatheit und Sicherheit

Christof Leng

Technische Universität Darmstadt
International Computer Science Institute Berkeley
cleng@icsi.berkeley.edu

Individuelle Privatsphäre und öffentliche Sicherheitsinteresse stehen scheinbar im ständigen Konflikt und müssen gegeneinander abgewogen werden. In der Tat benötigen Strafverfolgungsbehörden traditionell spezielle Privilegien zur Aufklärung von Straftaten, z.B. bei Wohnungsdurchsuchungen. Nicht immer kann jedoch durch weniger Privatheit mehr Sicherheit erreicht werden.

Durch den digitalen Wandel ergibt sich eine Vielzahl neuer Möglichkeiten für die Sicherheitsbehörden. Es sind nicht nur wesentlich mehr Informationen verfügbar, sondern sie sind auch in digitaler und vernetzter Form wesentlich leichter zu erlangen und automatisiert auswertbar. Ein fataler Teufelskreis führt dabei zur kontinuierlichen Aushöhlung der Bürgerrechte: Jeder Erfolg der Sicherheitsbehörden rechtfertigt die bestehenden Befugnisse; jeder Fehlschlag weckt und rechtfertigt hingegen weitergehende Befugnisse. Eine nüchterne Abwägung der Grundrechte gegeneinander ist unter diesen Umständen nicht möglich, und die einseitige Entwicklung bringt langfristig die freiheitlichen Grundfesten unserer Demokratie in Gefahr.

Bereits ein Konzept wie die Vorratsdatenspeicherung, welches von Strafverfolgern oft als unabdingbar dargestellt wird, widerspricht nach einheitlicher Rechtsprechung der Gerichte bereits in massiver Weise unserer demokratischen Grundordnung. Es zeigt sich jedoch, dass die Geheimdienste bereits seit Jahren eine sehr viel weitreichendere Totalüberwachung der Kommunikationsnetze praktizieren, weit jenseits der gesetzlichen Grundlagen und der demokratischen Kontrolle.

Diese Entwicklung entzieht sich trotz aller Enthüllungen weitgehend der öffentlichen Diskussion. Die Eingriffe in die Privatsphäre bleiben für den Einzelnen unbemerkt und zunächst ohne Folgen. Diese Unsichtbarkeit unterscheidet sich fundamental von anderen Formen staatlicher Gewalt und minimiert das Empörungs- und Betroffenheitspotential. Zum einen fühlt man sich nicht unmittelbar als Opfer, und zum anderen bleiben selbst drastische Fälle typischerweise ohne Gesicht. Wenn aber der ehemalige Ex-NSA-Chef Michael Hayden erklärt, „Wir töten auf Basis von Metadaten“, ist die Tragweite der Entwicklung kaum von der Hand zu weisen.

Zahlreiche Einzelfälle zeigen, dass die auf geheimen Überwachungsmaßnahmen basierenden Entscheidungen oft fehlerhaft aber gleichzeitig schwer anfechtbar sind. Das zentrale Problem ist jedoch, dass eine Infrastruktur geschaffen wird, deren Missbrauch in Krisenzeiten unmöglich zu verhindern ist und dann wesentlich zu einer Eskalation bei-

tragen könnte. Diese vermeintlichen Sicherheitswerkzeuge stellen somit selbst eine Gefahr für die individuelle und kollektive Sicherheit dar.

Folglich ist der Widerspruch zwischen Privatsphäre und Sicherheitsinteressen gar nicht so groß. Für die Sicherheit unserer freiheitlichen und demokratischen Gesellschaft ist die Privatheit kein Hindernis sondern eine Voraussetzung. Jeglicher Eingriff in die Privatsphäre muss daher offengelegt und äußerst sorgfältig abgewogen werden.

Daraus ergeben sich folgende Forderungen:

1. Grundrecht auf unbeobachtete Kommunikation

Die Meinungsfreiheit ist eine zentrale Stütze unserer Demokratie. Diese kann bereits vom Gefühl, überwacht zu werden, beeinträchtigt werden. Da ein stetig wachsender Anteil des innersten Lebensbereichs in den digitalen Netzen stattfindet, muss die Vertraulichkeit der ausgetauschten und gespeicherten Daten höchsten gesetzlichen Schutz genießen.

2. Keine verdachtsunabhängige Überwachung und Ausspähung

Die Unschuldsvermutung muss auch in der E-Society aufrechterhalten werden. Ohne einen konkreten und schwerwiegenden Anfangsverdacht darf das Grundrecht auf unbeobachtete Kommunikation nicht angetastet werden. Dies schließt insbesondere die flächendeckende Vorratsdatenspeicherung und Kommunikationsüberwachung, auch als Suche nach „verdächtigen“ Mustern, aus.

3. Dokumentations- und Offenlegungspflichten

Sollte aufgrund eines konkreten und schwerwiegenden Verdachts nach der Ausschöpfung anderer Ermittlungsmethoden eine richterlich angeordnete Überwachung oder Ausspähung notwendig geworden sein, muss diese nachvollziehbar dokumentiert und den Betroffenen zeitnah, z.B. nach Abschluss der Ermittlungen, angezeigt und offengelegt werden. Nur so kann die demokratiefeindliche Angst vor Überwachung minimiert werden.

4. Transparenz und Kontrolle der Behörden

Die Einhaltung der gesetzlichen Rahmenbedingungen durch die Sicherheitsbehörden ist derzeit faktisch nicht kontrollierbar. Eine personell angemessen und mit vollständigem Informationszugriff ausgestattete unabhängige Kontrollinstanz muss geschaffen werden, welche die demokratische Kontrolle der Sicherheitsbehörden wiederherstellt. Zudem müssen die vorhandenen Werkzeuge und Vorgehensweise der Sicherheitsbehörden der Öffentlichkeit transparent gemacht werden, um das Vertrauen wiederherzustellen und eine gesellschaftliche Kontrolle zu ermöglichen. Die IT-Security lehrt uns, dass transparente Methoden in der Praxis zuverlässiger sind als „security by obscurity“.

5. Unabhängige Überprüfung

Auch die Effektivität der Ermittlungswerkzeuge, welche durch die Einschränkung des Rechts auf Privatsphäre ermöglicht werden, muss regelmäßig von einer unabhängigen Stelle ermittelt und mit den möglichen Alternativen verglichen werden. Nur die Ergebnisse einer regelmäßigen objektiven Überprüfung können die Debatte wieder versachlichen.

6. Institutionelle Durchsetzung des Schutzes der Privatsphäre

Nicht zuletzt sollten die Sicherheitsbehörden den Schutz der Privatsphäre als wesentlichen Teil ihrer Aufgaben und des staatlichen Sicherheits- und Stabilitätsinteresses begreifen. Ein wesentliches Ziel muss daher die Sicherung der Privatsphäre gegenüber Kriminellen und sich außerhalb der eigenen Gerichtsbarkeit bewegenden Stellen fremder Staaten darstellen.