

Herr Präsident, hohes Gericht, sehr geehrte Damen und Herren,

Sechs Punkte zur Informations- und Kommunikationstechnik sind aus meiner Sicht besonders bedeutsam:

1. Moderne Speichertechniken (Bsp. USB-Stick, 32 GByte, 31,3 mm * 12,4 mm * 3,4 mm; <http://www.heise.de/preisvergleich/a457040.html>) ermöglichen
 - schier unbegrenzte Speicherung (im Beispiel: 20 mal alle Daten der Volkszählung von 1987),
 - effizientes Verstecken und Schmuggeln von Daten (wasserfest, vermutlich auch (magen)säurefest und damit auch schluckbar) und
 - kaum löschar.
2. Art. 10 GG muss inhaltlich erweitert und im Schutzniveau angehoben werden, da nicht-kommunikatives Verhalten von Menschen (z.B. Aufrufen des eigenen Terminkalenders; Nachschlagen in einem elektronischen Lexikon; digitale Bücher lesen) technische Kommunikationsvorgänge auslöst (so dass Menschen viel stärker darauf angewiesen sind, dem Kommunikationsgeheimnis vertrauen zu können, als bei ihnen bewusster Kommunikation, die sie auch vermeiden könnten). Art. 10 GG muss also aufgrund der technischen Entwicklung gestärkt und nicht durch Vorratdatenspeicherung weiter geschwächt werden.
3. Die Trennung von Verkehrsdaten/Protokolldaten einerseits und Inhaltsdaten der Kommunikation andererseits ist zunehmend unklar und deshalb kein für Grundrechtseinschränkungen geeignetes Unterscheidungskriterium. Sofern nicht überzeugend argumentiert werden kann, dass Verkehrsdaten/Protokolldaten auch künftig weniger sensible Daten sind als Inhaltsdaten, sollten

sie bzgl. Schutzniveau und Zugangsregeln wie Inhaltsdaten behandelt werden.

4. Die heute vorherrschende Unsicherheit großer Teile der eingesetzten Informationstechnik (IT) wird auch auf absehbare Zeit nicht deutlich reduziert werden können, d. h. jede durch IT für Befugte bereitgestellte Funktionalität wird auch von Unbefugten genutzt werden können: von Terroristen, von der Organisierten Kriminalität, von fremden (und nicht unbedingt nur: befreundeten) Geheimdiensten. Hieraus folgen zwei Empfehlungen:
 - Bestehende Sicherheitslücken der IT für Strafverfolgung und Verbrechensvorbeugung nutzen: Ja, wenn angemessen.
 - Weitere Sicherheitslücken (wie z. B. Vorratsdatenspeicherung) in IT einbauen: Nein!

Das vorgebrachte Argument, auch ohne Vorratsdatenspeicherung würden viele Daten zumindest kurzzeitig gespeichert, so dass die Vorratsdatenspeicherung die Situation zumindest nicht wesentlich verschlimmere, ignoriert die Mosaik-Theorie des Datenschutzes: Viele Daten zusammen sind viel sensibler als die einzelnen Daten. Mehr Daten zu speichern oder Daten länger zu speichern verschärft die Datenschutzproblematik also drastisch!

5. Terroristen und organisierte Kriminalität können der Vorratsdatenspeicherung so deutlich leichter und wirkungsvoller ausweichen als die demokratische Zivilgesellschaft, dass sich für die Vorratsdatenspeicherung nicht nur die Frage der Verhältnismäßigkeit stellt, sondern auch die Frage der Zweckeignung.
 - Spreizband-Funktechniken verhindern die Entdeckung, dass Kommunikation überhaupt stattfindet, und damit auch die Erfassung, wer wann mit wem von wo nach wo kommuniziert. Spreizband-

Funktechniken sind im militärischen Bereich üblich und deshalb sind entsprechende Geräte für Terroristen und organisierte Kriminalität beschaff- und nutzbar, da diese viel Geld pro Teilnehmer haben und zudem Kommunikation nur in kleinen geschlossenen Gruppen benötigen.

- Anonymisierungsdienste in Ländern, wo keine Vorratsdatenspeicherung erfolgt, lassen die Vorratsdatenspeicherung bezüglich all jenen weitestgehend leerlaufen, die sich schützen wollen und keine hohen Anforderungen an Durchsatz und Verzögerungszeit haben, wie dies z.B. bei E-Mail der Fall ist.

6. Überwachungsfreie Räume sind für Menschen als soziale Wesen notwendig (und technische Eliten werden sie sich und anderen im virtuellen Raum des „Internet“ sowieso schaffen). So zu tun, als sollte und könnte man überwachungsfreie Räume vermeiden, mag als Wahlkampfgetöse oder Interesse einzelner Bedarfsträger noch verständlich sein. Als Grundlage für die technische Infrastruktur einer demokratischen Informationsgesellschaft ist dies unakzeptabel.

Ich fasse zusammen: Vorratsdatenspeicherung von Kommunikationsdaten gefährdet und schwächt eine demokratische Gesellschaft deutlich. Sie ist aus technischer Sicht die unangemessenste aller in Diskussion befindlichen Maßnahmen im Bereich Strafverfolgung und Gefahrenabwehr.

Ich danke Ihnen für Ihre Aufmerksamkeit.

Andreas Pfitzmann

(Karlsruhe, 15. Dez. 2009)