Helmut Eiermann

Das IT-Grundrecht und seine Folgen

“Oft ist die Zukunft schon da, ehe wir ihr gewachsen sind.” Leicht kommt einem zur Informationstechnik diese Erkenntnis des Schriftstellers John Steinbeck in den Sinn. Die darin mitschwingende Besorgnis mag berechtigt sein, beim Grundrechtsschutz hat das Bundesverfassungsgericht jedoch Vorsorge getroffen.

Hintergrund

Auslöser des Bundesverfassungsgerichtsurteils vom 28.2.2008¹ waren die Regelungen in § 5 des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen, mit denen erstmals eine gesetzliche Ermächtigung für die Online-Durchsuchung, d.h. den verdeckten Zugriff auf fremde IT-Systeme, geschaffen wurde.

Die Sicherheitsbehörden trieb dabei die Sorge um, der technischen Zukunft nicht gewachsen zu sein. Die heimliche Untersuchung eines IT-Systems (Online-Durchsicht), die Erfassung von dessen Nutzung (Online-Überwachung) sowie der Datenzugriff vor einer ggf. verschlüsselt geführten Telekommunikation (Quellen-TKÜ) sollten wegbrechende Ermittlungsmöglichkeiten kompensieren.

Das Grundrecht

Das Bundesverfassungsgericht hat die besagten Regelungen für nichtig erklärt und neuartige Gefährdungen ausgemacht, denen mit dem bisherigen Grundrechtskanon nicht begegnet werden könne. Die „informationstechnischen Systemen“ anvertrauten Daten über die persönliche Lebensgestaltung erlaubten es, bei einer heimlichen Infiltration durch den Staat ein aussagekräftiges Persönlichkeitsbild einer Person zu gewinnen, dem vorhandene Grundrechte nicht ausreichend Schutz zu bieten vermögen. Die Möglichkeit entsprechender Eingriffe wurde von den Verfassungsrichtern nicht verworfen, jedoch an eindeutige Rechtsgrundlagen und sichernde Verfahrensregelungen geknüpft. Konkret hat das Bundesverfassungsgericht drei Schutzlücken ausgemacht:

- Das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) schütze ausschließlich Inhalt und Umstände einer laufenden Kommunikation, nicht jedoch Daten, vor Beginn des Kommunikationsvorgangs oder nach dessen Ende.
- Die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) erstrecke sich auf eine räumlich abgrenzbare Sphäre, in der sich das Privatleben entfaltet. Daten auf IT-Systemen außerhalb dieser Sphäre, wie sie sich z.B. aus der mobilen Nutzung oder der Speicherung im Internet, würden davon nicht erfasst.
- Das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG²) schütze vor einzelnen Datenerhebungen. Der heimliche Zugriff auf potentiell große und aussagekräftige Datenbestände, wie sie aus der Nutzung informationstechnischer Systeme resultierten, gehe in seinem Gewicht für

die Persönlichkeit des Betroffenen jedoch über einzelne Datenerhebungen hinaus und führe zu neuen Gefährdungen.

Den notwendigen Lückenschluss gewährleiste das Allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses schütze das Interesse des Nutzers daran, dass seine Daten vertraulich bleiben und Leistungen, Funktionen und Speicherinhalte nicht durch Dritte genutzt werden können.

Ausblick

Diese Herleitung hat bezüglich des letzten Punktes durchaus Kritik erfahren. Auch mag die vergleichsweise sperrige Formulierung des neuen Grundrechts denken lassen, dass es seinen Schutzbereich vorerst nur konturenhaft erkennen lässt. Das Bundesverfassungsgericht hat jedoch eine kluge Entscheidung getroffen: technikoffen, entwicklungsoffen und vorausschauend.

In erster Linie handelt es sich auch bei dem neuen IT-Grundrecht um ein Abwehrrecht gegenüber staatlichen Eingriffen; inwieweit es über die Drittwirkung seinen Weg in die Wirtschaft findet, wird sich zeigen. Ein Blick auf die Folgen des seinerzeit ebenfalls neuen Rechts auf informationelle Selbstbestimmung zeigt, dass dieses eine Reihe von Organisations- und Verfahrensnormen – auch außerhalb des staatlichen Bereichs – nach sich zog. Für das neue IT-Grundrecht ist Gleiches zu erwarten.

Wenngleich es sich bei Vertraulichkeit und Integrität vorliegend um verfassungsrechtlich zu interpretierende und nicht primär technische Begriffe handelt, sind Hashwerte, Verschlüsselung, Authentizitätsnachweise, Auditierung, Zertifizierung, Kennzeichnungspflichten, Prüf- und Revisionsmöglichkeiten Aspekte, in denen sich die konkrete Ausformung des IT-Grundrechts niederschlagen wird. Mit Anforderungen für staatliche Stellen, aber auch für die Betreiber von IT-Systemen.

Das Bundesverfassungsgericht hat es trotz einhegender Anforderungen zu Recht vermieden, den Begriff des „informationstechnischen Systems“ fest an technische Ausprägungen zu binden. Die Informationstechnik lässt Konzepte spiralförmig wiederkehren. Zentralisierung, Dezentralisierung, Endgeräteautarkie und Vernetzung sind Wiedergänger auf jeweils höherem technischen Niveau. Cloud Computing ist letztlich nichts anderes als die Rechenzentrumswelt der 70er Jahre mit ubiquitären Beigaben. Es spricht für die Weitsicht des höchsten deutschen Gerichts, die Notwendigkeit eines kohärenten Persönlichkeitsschutzes erkannt zu haben, damit dieser der Zukunft gewachsen ist, vielleicht sogar, bevor sie da ist.

¹ BVerfGE 120, 274 ff.

² BVerfGE 65, 1 Leitsatz Nr. 1