

Das Ende des Rechtsstaates aufgrund der digitalen Überwachung durch die Geheimdienste und die Auswirkungen auf den Datenschutz

Matthias Lachenmann



Nach dem Motto „Man braucht den Heuhaufen, um darin die Nadel zu finden“ (Keith Alexander) greifen die Geheimdienste westlicher Staaten (NSA, BND usw.) große Teile des weltweiten Internet-Verkehrs ab. So wird die Kommunikation von Regierungschefs ebenso wie die von einfachen Bürgern abgehört, Bewegungs- und Metadaten gespeichert, soziale Netzwerke gescannt und E-Mails anlasslos durchsucht und Inhaltsdaten gespeichert.

Diesen gravierenden Eingriffen in das Persönlichkeitsrecht stehen insbesondere zwei Urteile des Bundesverfassungsgerichts entgegen: Zum Einen das bereits 1983 ergangene sog. Volkszählungsurteil, in dem das allgemeine Persönlichkeitsrecht und, basierend auf Art. 2 Abs. 1 iVm 1 Abs. 1 GG, der Abwehrensanspruch des Bürgers gegen Ausforschung durch den Staat begründet wurde. Zum Anderen das Urteil des BVerfG zum sog. „Staatstrojaner“, in dem das Grundrecht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme begründet wurde.

Die Tätigkeiten der deutschen Geheimdienste sind zudem an Art. 10 GG zu messen. Grundsätzlich greift jede Kenntnisnahme und Verwertung von Kommunikationsdaten eines Bürgers in seine Rechte aus Art. 10 GG ein (BVerwG, Urt. v. 28.5.2014 – 6 A 1.13). Dabei bejaht das BVerfG einen weitreichenden Schutz (Urt. v. 14.7.1999 – 1 BvR 2226/94 u.a.) für personenbezogene Daten aller Bürger.

Das Datenschutzrecht, das im Bundesdatenschutzgesetz (BDSG) niedergelegt ist, erlangt beim Schutz gegen staatliche Ausforschung eine besondere Bedeutung. Zwar geht das BDSG von dem sog. Verbotsprinzip aus, also dem Verbot von Datenverarbeitung, soweit nicht eine Rechtfertigung vorliegt (§ 4 BDSG), allerdings gelangt dies kaum zu praktischer Bedeutung.

Relevant werden nunmehr Prinzipien, die bislang kaum praktische Bedeutung hatten: Bei Umsetzung des Prinzips der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) durch private Stellen können weniger Daten abgegriffen werden. Weiter sind von Bedeutung: Entnetzung, also die Trennung verschiedener Systeme, und die Information des Betroffenen. Besondere Bedeutung erlangt das Recht der Datensicherheit (§ 9 BDSG), das die zu ergreifenden technischen und organisatorischen Sicherungsmaßnahmen vorgibt. Auch das von der Bundesregierung geplante IT-Sicherheitsgesetz kann zum Schutze der Betroffenen dienen.

Die Geheimdienste überwachen auch Untersuchungsausschüsse, die die Handlungen dieser Geheimdienste untersuchen sollen (obwohl das Parlament die nachrichtendienstlichen Tätigkeiten gem. §§ 4 f. PKGrG überwachen soll und kann). Bürger, die sich mittels Verschlüsselung schützen wollen, werden als „Extremists“ geführt. Begründet wird dies mit der pauschalen Behauptung, der Schutz der „Sicherheit“ rechtfertige die (rechtswidrige) Einschränkung der Grundrechte. Diese Argumentation ist aus autokratischen Staaten bekannt und greift den Rechtsstaat in seinem Kern an.