In Kooperation mit:
**BITKOM -** Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
**davit im DAV -** Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein
**eco -** Verband der deutschen Internetwirtschaft e.V.
**VPRT -** Verband Privater Rundfunk und Telemedien e.V.

# MMR
# MultiMedia und Recht

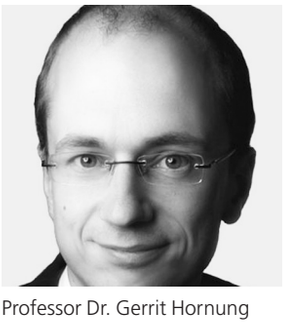
3/2015



EDITORIAL

## Die Krypto-Debatte: Wiederkehr einer Untoten

Die bisher letzte „Krypto-Debatte" (von einem „Krieg" soll hier nicht die Rede sein) ist so lange her, dass inzwischen eine ganze Generation von IT-Juristen, Informatikern und netzpolitisch Interessierten die Akteure, die Argumente und den Ausgang der damaligen Diskussion nur vom Hörensagen kennt oder sich dieser Tage erzählen lassen muss. Wiederkehrende Forderungen nach einem Verbot starker Verschlüsselungsverfahren, einem behördlichen Genehmigungsvorbehalt oder einer Pflicht zur Hinterlegung privater Schlüssel (Key Escrow) konnten sich letztlich weder in Deutschland noch in anderen westlichen Staaten durchsetzen. Hierzulande markierten die „Eckpunkte der deutschen Kryptopolitik" der *Bundesregierung* vom Juni 1999 das vorläufige Ende der Diskussion. Danach sollte die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland nicht eingeschränkt, sondern vielmehr ein Vertrauensrahmen für sichere Verschlüsselung geschaffen werden. Die *Bundesregierung* bekräftigte ihre Absicht, die internationale Wettbewerbsfähigkeit deutscher Hersteller für sichere und leistungsfähige Verschlüsselungsprodukte zu stärken. Hätte man irgendwann zwischen 1999 und Anfang 2015 die Altvorderen zu dieser Angelegenheit befragt – die einheitliche Auskunft wäre gewesen: Die Debatte ist tot, und zwar mausetot.



Professor Dr. Gerrit Hornung

Aber manchmal kehren die Untoten zu den Lebenden zurück. Nach den fürchterlichen Anschlägen auf das französische Satiremagazin Charlie Hebdo schlägt das Pendel in der Sicherheitsdebatte derzeit zu Gunsten neuer und bislang weithin abgelehnter Überwachungs- und Kontrollmechanismen aus. Hierzu gehört auch der durch den britischen Premierminister *Cameron*, US-Präsident *Obama*, EU-Anti-Terror-Koordinator *de Kerchove* und andere geforderte Einbau von „Hintertüren" in entsprechende Algorithmen oder die Hinterlegung privater Schlüssel bei staatlichen Behörden.

Die 20 Jahre alten Argumente gegen diese Ansätze sind heute so gültig wie damals; vielleicht sind sie sogar noch wichtiger geworden. Kryptografie ist in Zeiten weltweit vernetzter Infrastrukturen ein wichtiges – vielleicht das einzige – Instrument zum Schutz von persönlichen Daten ebenso wie von Betriebs- und Geschäftsgeheimnissen. Die Maßnahme ist angesichts der Verfügbarkeit vieler Verschlüsselungsprodukte aus dem In- und Ausland sowie von Open Source-Tools, aber auch wegen der Möglichkeiten der Verschleierung (Steganografie, Hinterlegung in Wirklichkeit nicht verwendeter Schlüssel) kaum

durchsetzbar und trifft deshalb maßgeblich gesetzestreue Bürger. Kryptografische Backdoors oder eine zentrale, durch den Staat oder in seinem Auftrag organisierte Datenbank mit privaten Schlüsseln wären ein gefundenes Fressen für die organisierte Kriminalität, Akteure der Wirtschaftsspionage oder ausländische Geheimdienste. Wegen der Vielzahl dieser negativen Effekte ist kaum vorstellbar, dass eine entsprechende Ermächtigungsgrundlage zum Eingriff in die betroffenen Kommunikationsgrundrechte verfassungskonform formuliert werden kann.

Legitime staatliche Sicherheitsinteressen sollten durch einzelfallbezogene, an konkrete Gefahren- oder Verdachtslagen anknüpfende Maßnahmen verfolgt werden. Dazu gehört in begründeten Fällen selbstverständlich auch der Zugriff auf internetvermittelte Kommunikation. Dieser wird durch den Einsatz von Kryptografie zwar komplizierter. Deren Verbot oder Schwächung ist aber keine verfassungsrechtlich verhältnismäßige Antwort auf dieses Problem. Die durch Bundesinnenminister *de Maizière* angesprochene Quellen-TK-Überwachung wirft zwar eigene Probleme auf (nicht zuletzt die umstrittene Frage der Ermächtigungsgrundlage, die de lege lata zu verneinen ist). Strukturell ist sie aber jedenfalls vorzugswürdig gegenüber Maßnahmen, die legitime Vertraulichkeitsinteressen der Bürger torpedieren – wie ein Verbot starker Kryptografie, eine Pflicht zur Schlüsselhinterlegung oder die durch *Edward Snowden* öffentlich gemachten Aktivitäten der *NSA* zur heimlichen Schwächung kryptografischer Algorithmen und Implementierungen.

Jede staatlich angeordnete Unsicherheit kryptografischer Produkte gefährdet die Geschäftsinteressen der Hersteller, weil das Vertrauen ihrer Kunden – mutmaßlich dauerhaft – zerstört wird. Ein wesentliches Ziel der im August 2014 vorgestellten „Digitalen Agenda" der *Bundesregierung* ist es, Deutschland zum „Verschlüsselungsstandort Nummer 1" zu machen. Will man diesen Weg blockieren, bevor die ersten echten Schritte auf ihm gemacht sind – eine neue Krypto-Debatte wäre der perfekte Mechanismus.

Die wirtschaftlichen Auswirkungen reichen aber weiter: Ein Staat, dessen Wirtschaft dermaßen auf die Entwicklung und den Schutz innovativer Ideen angewiesen ist wie Deutschland, muss ein höchstes Interesse an der Verfügbarkeit sicherer, bezahlbarer und leicht zu handhabender Verschlüsselungsverfahren haben. Ohne diese können technische Innovationen wie der Einsatz von cyber-physischen Systemen in der produzierenden Industrie („Industrie 4.0") nicht sinnvoll eingesetzt werden. Es verwundert deshalb nicht, dass die einschlägigen Branchenverbände der Wirtschaft praktisch unmittelbar die politischen Vorstöße abgelehnt haben. Auch die *Gesellschaft für Informatik* (*GI*) warnt, jegliche Beschränkung der Verschlüsselung inklusive einer staatlichen Schlüsselverwaltung führe zu einem Verlust von Vertraulichkeit und Sicherheit der Internetkommunikation. Jeder Bürger und jedes Unternehmen müsse aber uneingeschränkt vertraulich und integer digital kommunizieren können. Wichtige Transaktionen seien im Internet ohne starke, asymmetrische Kryptografie gar nicht denkbar.

Eine Pflicht zur Hinterlegung privater Schlüssel hat darüber hinaus eine verfassungsrechtliche Dimension. Auch diese wurde bereits vor 20 Jahren erkannt. Eine Beurteilung am Maßstab der seitdem ergangenen Rechtsprechung des *BVerfG* ist jedoch bislang noch nicht einmal in Ansätzen erfolgt. Da mithilfe der Schlüssel zu einem späteren Zeitpunkt der Zugriff auf sensible Kommunikationsinhalte ohne Wissen oder Kenntnisnahme der Betroffenen möglich ist, ist die Vertraulichkeit der Kommunikation unmittelbar gefährdet. Auf Grund der potenziellen Heimlichkeit der Maßnahme ist schon in der Hinterlegungspflicht ein Eingriff in das grundrechtlich geschützte TK-Geheimnis nach Art. 10 GG (bei verschlüsselten Speicherinhalten überdies in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, bei Betriebs- und Geschäftsgeheimnissen in Art. 12 und Art. 14 GG) zu sehen. Eine etwaige Hinterlegung bei einer privaten Stelle würde daran ebenso wenig etwas ändern wie die Tatsache, dass die Kommunikationsinhalte nur in einer kleinen Zahl von Fällen zur Kenntnis genommen würden. In ihren Urteilen zu der strukturell vergleichbaren Situation der Vorratsdatenspeicherung haben das *BVerfG* und der *EuGH* ebenfalls schon in der Speicherung der Daten einen Eingriff gesehen.

Im Rahmen der Verhältnismäßigkeitsprüfung sind die mit der Maßnahme verfolgten – legitimen – Sicherheitsinteressen den genannten Risiken gegenüberzustellen. Vor dem Hintergrund der genannten Urteile ist es kaum vorstellbar, dass diese Hürde in Deutschland oder in Europa genommen werden kann. Die Streubreite der Maßnahme wäre mutmaßlich vergleichbar. Anders als bei der Vorratsdatenspeicherung würden aber sogar Inhalte der Kommunikation zur Kenntnis der Behörden gelangen – einschließlich Gesundheitsdaten, Redaktionsgeheimnissen und Anwaltskommunikation.

Aus grundrechtlicher Perspektive sollte umgekehrt erkannt werden, dass den Staat eine Gewährleistungsverantwortung für eine vertrauliche und integre elektronische Kommunikation der Bürger trifft. Der Entwurf für ein IT-Sicherheitsgesetz (dessen Einzelheiten hier nicht diskutiert werden sollen) nimmt diesen Gedanken für den Bereich der kritischen Infrastrukturen auf. Es wäre geradezu grotesk, zum selben Zeitpunkt – gleich ob durch nationale Regelungen oder über den europäischen Umweg – durch staatliche Maßnahmen den Bürgern die Kryptografie als wesentliches Instrument des Selbstdatenschutzes aus der Hand zu schlagen.

Wiedervorlage: in 15 Jahren – gerne auch später.

Passau, im März 2015

**Professor Dr. Gerrit Hornung**
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik sowie Sprecher des Instituts für IT-Sicherheit und Sicherheitsrecht (ISL) an der Universität Passau.