expertenReport

Quelle: Adobe

13 Billionen Anfragen unter GeneralverdachtDNS-Überwachung ohne Grenzen? – Warum das BVerfG im Fall 1 BvR 2317/25 eine digitale Systemfrage stellt

Dirk Pappelbaum

Am 25. November 2025 hat das Bundesverfassungsgericht in einer einstweiligen Anordnung die Vollziehung eines amtsgerichtlichen Beschlusses zur DNS-Überwachung gestoppt. Was nach einem Nischenthema für Juristen klingt, betrifft in Wahrheit die Infrastruktur des Internets – und damit jeden Menschen, der heute online ist.

Was hier angeordnet wurde, war keine klassische Telekommunikationsüberwachung, sondern die flächendeckende Analyse der DNS-Infrastruktur – des „Telefonbuchs des Internets“. Und sie betrifft ein Grundrecht, das in digitalen Zeiten neu konturiert wird: das Fernmeldegeheimnis. (BvR 2317/25)

Was ist DNS und warum ist es sensibel?

Das Domain Name System (DNS) übersetzt menschenlesbare Internetadressen in technische IP-Adressen. Diese DNS-Anfragen laufen im Hintergrund bei jedem Webseitenaufruf, bei E-Mails, bei Updates oder API-Zugriffen. Sie sind damit ein digitaler Schatten des Nutzerverhaltens – lückenlos, unspektakulär, aber entlarvend.

Wer DNS-Anfragen zentral überwacht, kann Kommunikationsbeziehungen rekonstruieren, Interessenprofile ableiten und Verhaltensmuster erkennen – oft ohne inhaltlichen Zugriff auf Nachrichten selbst. Gerade weil DNS-Daten nicht verschlüsselt sind und standardmäßig an die DNS-Server des Internetanbieters gesendet werden, sind sie technisch leicht zugänglich – aber rechtlich besonders sensibel.

Im verhandelten Fall sollten nicht nur einzelne Verbindungen, sondern sämtliche DNS-Anfragen aller Kunden überwacht werden – um nach einer einzigen Zieladresse zu filtern. Die Maßnahme glich somit nicht der gezielten Suche nach einer Nadel im Heuhaufen, sondern der vollständigen Durchleuchtung des gesamten Heus.

Strukturbruch: Ermittlungsmaßnahme im Maßstab der Infrastruktur

Was das BVerfG zu Recht zurückweist, ist die strukturelle Entgrenzung der Maßnahme. Es geht nicht um den Einzelfall, sondern um die Reichweite des Eingriffs: Millionen unbeteiligte Kunden, keine informierte Einwilligung, keine Möglichkeit der Gegenwehr, keine nachträgliche Benachrichtigung – ein verdeckter Massenangriff auf das Fernmeldegeheimnis.

Das Gericht erkennt das technische Verhältnis: DNS-Anfragen sind nicht optional, sondern Voraussetzung jeder digitalen Kommunikation. Wer sie überwacht, greift tief in die Grundrechte ein – selbst wenn keine Inhalte erfasst werden. Die Richter betonen, dass solche Eingriffe nicht nur technisch umsetzbar, sondern auch rechtlich kontrollierbar sein müssen. Maßstab ist dabei nicht das Ermittlungsinteresse, sondern die verfassungsrechtliche Zumutbarkeit.

Rolle der Anbieter: Zwischen Umsetzungspflicht und Verfassungsauftrag

Bemerkenswert ist auch die Perspektive auf die Rolle der Telekommunikationsanbieter. Bisher galt vielfach: Wer zur Mitwirkung an einer Ermittlungsmaßnahme verpflichtet wird, hat diese zu erfüllen – nicht zu hinterfragen. Doch das Bundesverfassungsgericht betont, dass auch Anbieter Grundrechtsträger sind – und sich gegen übergriffige Maßnahmen zur Wehr setzen dürfen.

Im vorliegenden Fall trugen die Unternehmen vor, dass die Maßnahme nicht nur technisch aufwendig, sondern auch reputationsschädlich sei. Denn im Fall eines späteren Erfolgs der Verfassungsbeschwerde hätten sie eine verfassungswidrige Überwachung umgesetzt. Der Eingriff hätte zudem irreversible Folgen gehabt: Nicht nur durch die Erhebung, sondern durch die stille Tiefe des Zugriffs, der weder den Betroffenen noch der Öffentlichkeit kommuniziert worden wäre.

Verhältnismäßigkeit im digitalen Maßstab

Die Entscheidung ist kein finales Urteil über die Rechtmäßigkeit der Maßnahme, sondern eine vorläufige Regelung im Eilverfahren. Doch sie setzt Maßstäbe: Die Richter legen dar, dass bei unklarer Rechtslage der potentielle Schaden für Grundrechte schwerer wiegt als das Strafverfolgungsinteresse – zumal alternative Ermittlungsmethoden weiterhin verfügbar sind.

Damit stellt das Gericht eine klare Strukturregel auf: Digitale Eingriffe, die in ihrer Architektur massenhaft und tiefgreifend sind, bedürfen einer besonders sorgfältigen rechtlichen Begründung. Nicht die technische Möglichkeit rechtfertigt den Eingriff, sondern die rechtsstaatliche Notwendigkeit.

Zwischen Aufklärung und Kontrolle

Die Digitalisierung macht neue Ermittlungsformen möglich – und gefährlich. Wer DNS-Daten als Ermittlungsquelle nutzen will, muss erkennen: Sie sind Teil der kritischen Infrastruktur unserer Kommunikationsfreiheit. Eine flächendeckende DNS-Überwachung kann technisch leicht aussehen – ist aber verfassungsrechtlich schwerwiegend.

Das Bundesverfassungsgericht signalisiert mit seiner Anordnung, dass es nicht nur die Maßnahme selbst, sondern auch die dahinterstehende Systemlogik prüft: Skalierung darf nicht als Rechtfertigung dienen. Es geht nicht nur um Datenschutz – sondern um Struktur, Steuerung und Vertrauen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4947366/bverfg-dns-ueberwachung-2025/