

## Online-Durchsuchung - warum nicht?

Sven Lüders

Fünf gute Gründe gegen eine Legalisierung der Online-Durchsuchung von Computern

### **1. Die Online-Durchsuchung gewährleistet keinen absoluten Schutz des Kernbereichs privater Lebensgestaltung**

Mit seinen Entscheidungen zum Großen Lauschangriff (3. März 2004) und zur präventiven Überwachung der Telekommunikation (27. Juli 2005) hat das Verfassungsgericht bekräftigt, dass es einen absolut geschützten Kernbereich privater Lebensgestaltung geben muss, in den der Staat unter keinen Umständen eingreifen darf. Dieser absolut zu sehende Schutz bedeutet, dass über derartige Verhaltensweisen weder Informationen erhoben, gespeichert noch verarbeitet werden dürfen.

Ein solcher Schutz der Privatsphäre ist bei einer Online-Durchsuchung nicht zu gewährleisten. Nach den Vorstellungen der Sicherheitsbehörden sollen die Zielrechner automatisch durchsucht, die „verdächtigen“ Daten dann zur Auswertung verdeckt an die Behörden übertragen werden. Eine automatisierte Suche kann aber nur syntaktischen Regeln folgen (z.B. Stichwortlisten oder Dateiendungen). Ob dabei Informationen aus dem Kernbereich privater Lebensgestaltung erfasst werden, lässt sich nur im Nachhinein, durch eine menschliche Interpretation der ermittelnden Beamten erkennen.

### **2. Die Online-Durchsuchung ist kein geeignetes Instrument der Strafverfolgung**

Im Gegensatz zu einer Beschlagnahme von Computern, bei der die Datenträger physisch durch die Ermittlungsbeamten sichergestellt werden, zielt die Online-Durchsuchung darauf ab, heimlich an Kopien dieser Daten zu gelangen. Derartige Kopien von digitalen Daten genügen nicht den Anforderungen an die Beweissicherheit, da sie für Übertragungsfehler oder unbeabsichtigte Veränderungen anfällig sind.

Darüber hinaus ist die Urheberschaft der Daten, die bei einer Online-Durchsuchung gewonnen werden, äußerst fragwürdig. Im Zweifelsfall kann nicht geklärt werden, ob die inkriminierten Daten von dem Besitzer/Beschuldigten auf dem Computer hinterlassen wurden, oder ob sie gezielt oder zufällig von anderen in das System eingebracht wurden. Bei der mündlichen Verhandlung des Bundesverfassungsgerichts zur Online-Durchsuchung am 10.10.2007 in Karlsruhe räumten die Vertreter der Sicherheitsbehörden ein, dass sie erst dann, wenn sich der Zielrechner in ihrem Besitz befinde, zweifelsfrei wissen, ob sie den richtigen Computer durchsucht haben.

### **3. Die Online-Durchsuchung ist kein geeignetes Instrument für eine gezielte Gefahrenabwehr**

Von den Vertretern der Sicherheitsbehörden, u.a. dem Präsidenten des Bundeskriminalamtes Jörg Ziercke,

wird immer wieder betont, die Online-Durchsuchung werde zur Abwehr terroristischer Gefahren benötigt. Zugleich betonen diese Befürworter des heimlichen Spähangriffs auf private Rechner, die Anwendung komme nur in Einzelfällen in Betracht - allein schon deshalb, weil die Vorbereitung der Online-Durchsuchung so aufwändig sei und die Erkundung des (informationstechnischen) Umfeldes der Zielpersonen sowie die Anpassung der Software voraussetze.

Beim Vorliegen einer konkreten Gefahrenlage (d.h. es existieren konkrete Handlungs- und Zeitpläne für einen Anschlag) würde die Online-Durchsuchung regelmäßig zu spät kommen. In derartigen Situationen wäre polizeiliches Handeln geboten. Auf der anderen Seite bedeutet dies, die Online-Durchsuchung kann sich nur gegen Personen richten, gegen die nur vage Verdachtsmomente vorliegen, dass sie möglicherweise eine Straftat begehen werden.

#### **4. Die Online-Durchsuchung ist mehr als nur eine weitere heimliche Überwachungsform - sie entblößt unter Umständen die gesamte digitale Vergangenheit der Betroffenen**

Im deutschen Strafverfahrensrecht existieren zahlreiche [heimliche Ermittlungsmethoden](#), um einer Straftat verdächtige Personen zu observieren, zu belauschen und anderweitig zu überwachen. Solche verdeckten Ermittlungsmaßnahmen zielen auf das aktuelle Verhalten der Betroffenen. Bei einer Online-Durchsuchung werden jedoch - anders als etwa bei einer Telekommunikationsüberwachung - nicht nur laufende Kommunikationen und Verhaltensweisen überwacht. Mit dem Einsetzen der massenhaften Verbreitung von Computern als PCs werden immer mehr Dinge des alltäglichen Lebens über Computer abgewickelt - und bleiben dort im Zweifelsfall auch gespeichert. Mit dem heimlichen Zugriff auf den Datenbestand eines PCs gerät deshalb unter Umständen die gesamte „informationelle Historie“ eines Computernutzers ins Visier der Ermittler.

#### **5. Mit der Online-Durchsuchung gingen bisherige Standards des (nachträglichen) Rechtsschutzes verloren**

Bei der Online-Durchsicht von Daten besteht immer die Gefahr, dass die Ermittler persönlichste Dinge über den Betroffenen erfahren, also in dessen (intime) Privatsphäre eingreifen. Dies kann grundsätzlich auch bei einer offenen Durchsicht einer Wohnung geschehen. Zum Schutz vor solchen Übergriffen auf die Privatsphäre sieht die Strafprozessordnung zahlreiche Möglichkeiten vor, sich gegen eine Wohnungsdurchsuchung zu wehren. "Das Bild der Strafprozessordnung von einer rechtmäßigen Durchsicht ist dadurch geprägt, dass Ermittlungsbeamte am Ort der Durchsicht körperlich anwesend sind und die Ermittlungen offen legen ..." (BGH) Mit dieser Offenheit der Ermittlungen wird u.a. gewährleistet,

- dass der Betroffene selbst kontrollieren kann, ob die Beamten wirklich nur nach den Sachen suchen, die im Durchsuchungsbeschluss beschrieben sind
- dass der Betroffene Art und Dauer der Durchsicht selbst kontrollieren kann
- dass er vor Ort oder nachträglich einen Rechtsschutz gegen die Durchsicht und ggf. Beschlagnahme von Sachen einlegen kann.

All dies ist beim heimlich stattfindenden Durchsuchen und Kopieren gespeicherter Daten nicht möglich.

---

<https://www.humanistische-union.de/thema/online-durchsuchung-warum-nicht/>

Abgerufen am: 25.04.2024