

# Grosser Online-Lauschgriff?

*Die aktuellen juristischen Gutachten zur „Online-Durchsuchung“ sind sich in zwei Fragen einig: Technisch ist sie kaum machbar, und gegen sie sprechen schwer wiegende verfassungsrechtliche Bedenken. Das Bundesinnenministerium ficht das nicht an. Dessen Informationspolitik kann auch zu dem Fazit führen, dass die die Öffentlichkeit – wider besseres Wissen der Verantwortlichen – getäuscht werden soll.*

Der Dritte Strafsenat des Bundesgerichtshofs hat schon vor einem knappen Jahr die „verdeckte Online-Durchsuchung“ [verboten](#). In Kürze wird [entschieden](#), ob die Verfassungsbeschwerde gegen deren bisher einzige juristische Ermächtigungsgrundlage, das nordrhein-westfälische [Verfassungsschutzgesetz](#), Erfolg haben wird. Das Bundesverfassungsgericht wird über die so genannte „Online-Durchsuchung? jedoch nur indirekt urteilen. Im fraglichen Gesetz heißt es [wörtlich](#), es gehe um „heimliches Beobachten und sonstiges Aufklären des Internets, wie insbesondere die verdeckte Teilnahme an seinen Kommunikationseinrichtungen bzw. die Suche nach ihnen, sowie der heimliche Zugriff auf informationstechnische Systeme auch mit Einsatz technischer Mittel.“ Der Begriff „Online-Durchsuchung? kommt im Text gar nicht vor. Die Idee, die Strafverfolger und die Behörden würden auf privaten Rechnern heimlich Software installieren können, ist eine Erfindung der Medien, insbesondere der [Süddeutschen](#) (07.12.2006) und der [taz](#) (30.01.2007). Der polizeiliche „Hackerangriff“ hat sich jedoch im allgemeinen Sprachgebrauch und seit dem Medienhype vor einem Jahr auch als Wunschvorstellung in der Politik eingebürgert.

[Ulf Buermeyer](#), wissenschaftlicher Mitarbeiter beim Bundesverfassungsgericht, hat im August 2007 in einem [Aufsatz](#) umrissen, warum schon aus der vergangenen Rechtsprechung abgeleitet werden kann, dass ein heimlicher Zugriff des Staates auf private Rechner, wie von Schäuble befürwortet,

schlicht verfassungswidrig ist. Unter „Zugriff? kann man verstehen, mit Hilfe technischer Mittel den Rechner eines Verdächtigen – ohne dessen Wissen – über einen bestimmten Zeitraum zu überwachen, auch ohne dass die dazu notwendige Software „online? implementiert werden müsste. Das ist ohnehin noch nie erfolgreich geschehen, trotz gegenteiliger Meldungen in den Medien, und auch äußerst unwahrscheinlich, da sich jeder dagegen mit einfachen Mitteln schützen könnte.



Buermeyer zweifelt in seinem Text „Die „Online-Durchsuchung“. Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme? nicht nur daran, dass die Ermittlungsmethode der Online-Durchsuchung „jemals effektiv wird angewendet werden können?, sondern führt zwei gewichtige juristische Argumente an, die das Bundesverfassungsgericht zu erwägen habe – die Unverletzlichkeit der Wohnung nach Artikel 13 Absatz 1 des Grundgesetzes und den so genannten „Kernbereichsschutz“ privater Lebensgestaltung. Interessant ist der Aufsatz Buermeyers vor allem deshalb, weil er beweist,

dass das Bundesverfassungsgericht seine bisherige Rechtsprechung über den Haufen werfen müsste, erlaubte es das, was dem Bundesinnenministerium vorschwebt (zum Beispiel in den [„Fragen und Antworten“](#) zur Online-Durchsuchung“.

Das Bundesverfassungsgericht hat am 3. März 2004 zum „Großen Lauschangriff“ [geurteilt](#), das Grundrecht auf Unverletzlichkeit der Wohnung meine nicht nur den Schutz vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt in allen Räumen, die privat und beruflich genutzt werden – inklusive Keller, Balkon und Garten, ja sogar ein zeitweilig genutztes Hotelzimmer. Es ging noch viel weiter:

*„Die heutigen technischen Gegebenheiten erlauben es, in die räumliche Sphäre auch auf andere Weise einzudringen. Der Schutzzweck der Grundrechtsnorm würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung des Absatzes1 umfasst wäre.“*

Die wenigen Juristen, die eine heimliche „Online-Durchsuchung“ für unbedenklich halten, kommen um diese Argumentation des Bundesverfassungsgerichts nicht herum. Die Wohnung ist sakrosankt, und was das Bundesverfassungsgericht einmal entschieden hat, besitzt quasi Gesetzeskraft. Man kann das nur durch verbale Taschenspielertricks umgehen. Einige Juristen konstruieren um den Computer einen „virtuellen Raum“, der mit einem Online-Anschluss entstehe und der daher nicht mehr zur „Wohnung“ gehöre (vgl. [Beulke/Meininghaus](#): „Anmerkung zur Entscheidung des BGH vom 21.2.2006 StV 2007, S. 63 ). Noch abwegiger ist zum Beispiel die These, derjenige, der sich des Internet bediene, wüsste, dass sein Computer „hierdurch vielfältigen Angriffen durch Würmer usw.“ ausgesetzt sei. Der Nutzer nehme das somit in Kauf, öffne sein System selbst und begeben sich damit in die „Sozialsphäre“, die keine „Wohnung“

mehr sei. Dr. Jürgen P. Graf, damals Oberstaatsanwalt beim Bundesgerichtshof, meinte noch 1999 in der Deutschen Richterzeitung, der Anbieter von Daten erkläre sich mit der Eröffnung des freien Zugangs im Internet „mit dem Zugriff durch beliebige Dritte? automatisch einverstanden. Mit dem technischen Sachverstand der meisten Juristen ist es ohnehin nicht sehr weit her. Die überwiegende Anzahl der Autoren nimmt es unkritisch als Tatsache hin, dass ein – wie auch immer gearteter – „Bundestrojaner“ technisch umsetzbar sei. Man könnte auf ähnlichem Niveau auch darüber diskutieren, ob der Einsatz einer Tarnkappe – wie im Nibelungenlied – für Polizisten der Verfassung entspräche.

Buermeyer aber war Netzwerk-Administrator der Universität Leipzig und ist daher eine Ausnahme. Die zweite Säule seiner Argumentation, warum eine Online-Durchsuchung verfassungswidrig sei, ist der Schutz des Kernbereichs privater Lebensgestaltung. Der fußt auf der durch den Artikel 1 des Grundgesetzes geschützten unantastbaren Menschenwürde. Noch nicht einmal der Bundestag könnte diesen Artikel mehrheitlich abschaffen oder verändern:

*„Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken. Gleichwohl ist bei staatlichen Beobachtungen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen. Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen*

*Strafverfolgungsinteresse.“*

In diesem „Kernbereich“ darf der Staat noch nicht einmal Daten erheben. Das hat das Bundesverfassungsgericht eindeutig formuliert und damit auch allen Ideen eines „Richterbands“ oder „Richtervorbehalts“ eine Absage erteilt. Für die Online-Durchsuchung heißt das: Da es keine technische Möglichkeit gibt, auf einem Rechner vorab „private“ Daten, die unter diesen „Kernbereich“ fallen, von denen zu trennen, für die das eventuell nicht zutrifft, verbietet sich der Einsatz heimlicher staatlicher Schnüffel-Software sogar bei Keyloggern.



Das Bundesinnenministerium müsste genug sachverständige Experten haben, die sowohl die juristische Argumentation als auch die technischen Implikationen nachvollziehen könnten. In den „Fragen und Antworten zur Online-Durchsuchung“, die mittlerweile auch auf der Website des Bundeskriminalamts verlinkt ist, wird jedoch das Gegenteil suggeriert. Auf das Urteil des Bundesgerichtshofs gegen die Online-Durchsuchung wird mit keinem Wort eingegangen, bloße technische Spekulationen werden für bare Münze ausgegeben:

*„Bevor eine Online-Durchsuchung durch Beamte des*

*Bundeskriminalamts (BKA) durchgeführt wird, prüft ein unabhängiger Richter grundsätzlich, ob diese Durchsuchung auf einem PC einer Privatperson oder in einer Firma durchgeführt werden darf.“ (...) Die Ermittlungs-Software wird nicht zu einer Beeinträchtigung der auf dem betroffenen Rechner installierten Sicherheitssoftware führen. (...) Sollte die Software dennoch entdeckt werden, wird sie vom Zielsystem entfernt.“*

Diese drei Thesen haben weder eine rechtliche Grundlage noch sind sie als unverbindliche Idee gekennzeichnet. Technisch erscheinen sie ohnehin als unsinnig. Eine derartige Software – inklusive einer Art Selbstzerstörungsmechanismus und der Möglichkeit, gerichtfeste Daten zu bekommen – gibt es noch nicht und wird es wohl auch nicht geben. Das [Gutachten](#) Prof. Ulrich Siebers zum Beispiel bekräftigt das differenziert: „Nach den Standards für digitale Forensik ist die Analyse eines im Betrieb befindlichen Systems problematisch, da ständig Daten verändert werden.“ Falls die Daten einen dümmsten anzunehmenden Kriminellen „online“ zu den Strafverfolgern gelangten, hätte die Staatsanwaltschaft größte Probleme, deren Authentizität zu beweisen.

Das Bundesinnenministerium verweigert über den technischen Hintergrund jede Auskunft. Auch auf einfache Fragen erhält man keine Antwort, zum Beispiel:

„Ist Ihnen bekannt, dass sich jeder Computer-Nutzer leicht dagegen schützen kann, dass ihm unbemerkt Fremdsoftware auf den Rechner „gespielt“ wird, wenn man sich an die [Ratschläge](#) des Bundesamtes für Sicherheit in der Informationstechnik hält? Wie kann verhindert werden, dass Terroristen die Ratschläge des BSI zum Thema Internet-Sicherheit beherzigen? Ist ihnen bekannt, dass bis jetzt in Deutschland noch kein erfolgreicher Versuch seitens des Bundeskriminalamtes und des Verfassungsschutzes (nach dessen eigenen Angaben) stattgefunden hat, einem Verdächtigen ohne dessen Wissen eine



Software auf den Rechner zu spielen, um einen so genannten Remote-Access-Zugang zu erhalten? Haben Sie vor der Veröffentlichung „Fragen und Antworten zum Thema Online-Durchsuchungen“ den Rat Sachverständiger eingeholt, ob eine Online-Durchsuchung überhaupt technisch umsetzbar sei? Was veranlasst Sie zu der Annahme, das sei zukünftig der Fall?

Markus Beyer, Pressereferat des Bundesinnenministeriums antwortet nur:

*„Wie Sie wissen handelt es sich bei der geplanten sog. Onlinedurchsuchung, wie auch bei der geplanten Novelle des BKA-Gesetzes insgesamt, um einen laufenden Gesetzgebungsprozess auf Fachebene, der noch nicht abgeschlossen ist. Daher bitten wir um Verständnis, dass wir auf weitere Detailfragen derzeit nicht eingehen können. (...) Insbesondere darf ich darauf hinweisen, dass das Bundesverfassungsgericht allein über eine Regelung des Landes NRW (!) entscheidet. Die geplante Novelle des BKA-G ist nicht Gegenstand der Verhandlung beim Bundesverfassungsgericht.“*

Man tut also so, als ob das möglich sei. Und da das Bundesverfassungsgericht nur über das Verfassungsschutzgesetz eines Bundeslandes befinden will, macht man einfach so weiter, als gebe es die vergangene und aktuelle Rechtsprechung gar nicht. Der Verdacht drängt sich auf, dass man in Schäubles Haus schlicht keine Ahnung hat, wie man das gewünschte polizeiliche „Hacken? bewerkstelligen will. Nur völlig unerfahrene Computer-Nutzer sind durch die wolkigen Formulierungen zu beeindrucken, Terroristen vermutlich nicht.

Auch der bayerische Innenminister Joachim Herrmann forderte in einem

[Interview](#) „Online-Durchsuchungen“. Herrmann ist ebenfalls nicht in der Lage, auf nur eine der ihm gestellten Fragen substantiell zu antworten – weder auf die juristischen noch auf die technischen. Zum Beispiel:

„Auf Grund welcher Annahmen geht Herr Joachim Herrmann davon aus, dass es Zukunft eine funktionsfähige Methode zur „Online-Durchsuchung‘ privater Rechner geben wird?“

Oder: „Das Bundesverfassungsgericht hat in einer Entscheidung zum Niedersächsischen Polizeigesetz seine Feststellungen aus dem Jahre 2004 zum Schutz des Kernbereichs privater Lebensgestaltung vor Eingriffen des Staates nochmals verdeutlicht. Das Gericht hebt hervor, ein Erhebungsverbot bestehe, wenn in einem konkreten Fall Anhaltspunkte vorliegen, dass eine Überwachungsmaßnahme Inhalte erfassen könne, die zu dem definierten Kernbereich gehören. Frage: Wie kann der Schutz des Kernbereichs privater Lebensgestaltung garantiert werden, wenn eine Software auf dem Rechner des Verdächtigen ohne dessen Wissen installiert worden ist?“

Die lapidare Antwort – per Word-Attachment – von [Karl Michael Scheufele](#), dem Pressesprecher des Bayerischen Staatsministeriums des Innern: „Moderne Kommunikationstechnik darf nicht die Folge haben, dass Terroristen rechtsfreie Räume für Verbrechensplanung haben. Wenn solche Organisationen sich dieser Kommunikationsmittel bedienen, dann müssen die Sicherheitsbehörden die Möglichkeiten haben, darauf zu reagieren. Selbstverständlich werden die verfassungsrechtlichen Vorgaben des BverfG eingehalten.“





Man darf getrost annehmen, dass hier der Wunsch der Vater des Gedankens ist. Aber die Leitmedien argumentierten beim Thema auch nicht gehaltvoller als die Politiker. Auf der Website der Tagesschau wird seit Monaten eine [Infografik](#) präsentiert, die suggeriert, eine Online-Durchsuchung würde im Sinne Schäubles schlicht funktionieren, ohne die skeptischen Einwände der IT-Fachleute auch nur ansatzweise zu berücksichtigen. Der Redaktion von tagesschau.de gelang es im Lauf einer Woche nicht, trotz mehrmaliger Anrufe und einiger E-Mails, den zu benennen, der die Infografik erstellt hatte.

„Ist tagesschau.de bekannt, dass es bis jetzt noch keine einzige erfolgreiche Online-Durchsuchung gegeben hat? Was veranlasst tagesschau.de anzunehmen, dass die in der Info-Grafik vorgestellten „Methoden“ umsetzbar und praktikabel seien?“

Auch darauf gab es keine Antwort. Was zu beweisen war.

*Dieser Artikel erschien leicht gekürzt am 28.01.2008 in*

Telepolis. Fotomontagen: Burks mit Material des Bundestags und der Tagesschau.