



Literatur

KEPPLINGER, HANS MATHIAS (1998): The Transformation of Politics Through the Development of the Mass Media. In: Giessen, Hans W. (Ed.): Long-Term Consequences on Social Structures through Mass Media Impact. Berlin: Vistas 1998, 109–119.

VIALON, PHILIPPE (2005): L'interculturalité dans la communication médiatique aujourd'hui : quelque chose de nouveau à l'ouest ? In: Fischer, Carolin; Harth, Helene; Vialon, Philippe & Virginie (Hg.): Identität und Diversität. Eine interdisziplinäre Bilanz der Interkulturalitätsforschung in Deutschland und Frankreich – Identité et diversité. Etat des lieux interdisciplinaire de la recherche sur l'interculturalité en France et en Allemagne. Berlin: Avinus 2005.

Der Autor

Hans Giessen

Studium an der FU Berlin, der Universität de Metz und der Universität des Saarlandes, Saarbrücken; Promotion. Berufstätigkeit im Medienbereich, Saarbrücken und Luxemburg. Wissenschaftliche Tätigkeit an der Universität des Saarlandes und an verschiedenen deutschen, englischen, französischen und schweizer Hochschulen, derzeit Privatdozent an der Universität des Saarlandes.



Informantenschutz in Zeiten der Online-Durchsuchung

Deutsche Ermittlungsbehörden wollen die Festplatten von Rechnern durchleuchten können. Damit ist nicht nur der Informantenschutz, sondern auch die Pressefreiheit als solche unmittelbar gefährdet.

Unter einer heimlichen Online-Durchsuchung wird die Möglichkeit der Ermittler verstanden, verdeckt über eine sogenannte Remote-Forensic-Software Zugriff auf ein informationstechnisches System zu erlangen und dort gespeicherte Daten online abzusaugen. Die Software erlaubt die Fernbedienung und damit die Fremdkontrolle des Zielcomputers. Als Zugriffs- bzw. Infiltrationsmethode wurden bisher technisch und juristisch vor allem das Zuspielden der Software via E-Mail-Anhang oder zugespieltem Datenträger diskutiert.¹ Theoretisch ist eine Online-Durchsuchung so machbar. Der Zugriff würde aber nur dann von Erfolg gekrönt sein, wenn die Ermittler tatsächlich den „Bundestrojaner“ auf dem richtigen Rechner installieren könnten und der Zugriff fortan unbemerkt bliebe. Beides setzt umfassende Kenntnis des zu durchsuchenden Systems voraus. Und beides setzt voraus, dass der Betroffene keine Schutzmaßnahmen ergriffen hat.

Die Geschichte der Online-Durchsuchung

Der mediale Hype um die Online-Durchsuchung begann Ende 2006 mit einem Bericht von Annette Rammelsberger in der Süddeutschen Zeitung: Die Sicherheitsbehörden seien längst dabei, private Festplatten auszuspionieren.² Das ist nicht der Fall. Nach zwei Jahren Behauptungen und Spekulationen gibt es einen einzigen Fall einer



Foto: Picture Alliance; Fotograf: Jens Becker

Auch Journalisten sind vor dem staatlichen Datenhunger längst nicht mehr sicher

Online-Durchsuchung, der sich nicht ohne Weiteres falsifizieren lässt. Der in Berlin lebende deutsche Staatsangehörige ägyptischer Herkunft Reda Seyam, der als „Gefährder“ gilt und seit Längerem durch mehrere Geheimdienste überwacht worden sein soll, behauptete, trotz anschlagentem Virenschanner einen E-Mail-Anhang geöffnet zu haben. Den Ermittlern waren zudem durch die Beobachtung der Computer, das verwendete Betriebssystem und der Standort des Rechners bekannt.³ Das war erforderlich, damit die Maßnahme gelingen konnte. Alle anderen angeblichen Online-Durchsuchungs-Fälle sind faktisch keine Online-Durchsuchungen im beschriebenen Sinne gewesen oder Falschmeldungen bzw. „missverständlich ausgedrückte“ Nachrichten.⁴



Die Entscheidung des Bundesverfassungsgerichts

Das Bundesverfassungsgericht hatte im Februar 2008 über die Online-Durchsuchung zu entscheiden. Es leitete zunächst die „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ aus dem allgemeinen Persönlichkeitsrecht ab.⁵ Damit wurde der Grundrechtsschutz und damit der Schutz vor dem staatlichen Zugriff entsprechend der technologischen Entwicklung und der zunehmenden Verbreitung informationstechnischer Systeme ergänzt und angepasst. Die Karlsruher Richter stellten außerdem klar, dass die Online-Durchsuchung als staatliche Maßnahme einen Eingriff in eben diese neue Gewährleistung darstellt. Damit genießen auch die statischen Daten auf einer Festplatte Grundrechtsschutz.⁶ Daten eines Kommunikationsprozesses bleiben dagegen weiterhin durch das Fernmeldegeheimnis des Art. 10 Absatz 1 Grundgesetz geschützt.⁷

Grundrechtseingriffe können allenfalls im Rahmen der im Grundgesetz oder durch die verfassungsrichterliche Rechtsprechung festgelegten Gründe gerechtfertigt werden. Da die Online-Durchsuchung elementar in das gewährleistete Grundrecht eingreift und zudem die Gefahr eines umfassenden Persönlichkeitsprofils in sich birgt, verlangen die Verfassungshüter enge Voraussetzungen für eine Rechtfertigung der Online-Durchsuchung. Die Online-Durchsuchung sei nur dann mit dem Grundgesetz vereinbar, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr für „überragend wichtige Rechtsgüter“ gegeben seien. „Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt.“⁸

Die Online-Durchsuchung bedarf einer vorherigen richterlichen Genehmigung.

Durch diesen sogenannten Richtervorbehalt sollen die Rechte des Betroffenen, der von der verdeckt durchgeführten Maßnahme nichts weiß, stellvertretend durch den Richter verfahrensrechtlich abgesichert werden.⁹ Bei der automatisierten Datenabschöpfung wissen die Ermittler außerdem nicht, ob sie auch solche Daten erfassen, die dem durch die Menschenwür-

Das alles hindert die Politik nicht daran, weiterhin lautstark und für alle Sicherheitsbehörden die Online-Durchsuchung zu fordern.

de-Garantie gewährleisteten absolut geschützten privaten Rückzugsraum – der sogenannte Kernbereich privater Lebensgestaltung – zuzurechnen sind. Solche Daten dürfen grundsätzlich weder erfasst und erst recht nicht verwertet werden. Sie sind für die Ermittler tabu. Aufgrund der technischen Eigenart der Online-Durchsuchung bei der Erfassung verlangen die Karlsruher Richter deshalb ein zweistufiges Schutzsystem für den Kernbereich der privaten Lebensgestaltung. In der ersten Stufe soll durch vorangehende Ermittlungen so weit wie möglich verhindert werden, dass Daten, die diesem absolut geschützten Kernbereich privater Lebensgestaltung zuzurechnen sind, überhaupt erfasst werden. Da es bedingt durch die Technik aber regelmäßig nicht ausgeschlossen werden kann, dass solche Daten dennoch erfasst werden, haben im Anschluss an die Maßnahme zunächst unabhängige Prüfinstanzen die erfassten Daten auf den Kernbereichsbezug zu überprüfen. Diskutiert wird hierbei vor allem das sogenannte Richterband, also die Vorabdurchsicht durch einen unabhängigen Richter. Sind die Daten freigegeben, stehen sie den Ermittlungsbehörden zur Verfügung.¹⁰

Das Bundesverfassungsgericht hat mitnichten die dritte Infiltrationsmethode – den physischen Zugriff durch Betreten der Wohnung – als notwendige Begleitmaßnahme zugelassen.¹¹ Es hat sich auch nicht dazu geäußert, wie es verfassungsrechtlich zu bewerten ist, wenn die Ermittler die Daten nicht nur kopieren, sondern auch aktiv und vorsätzlich Daten verändern oder löschen.¹² Eine abschließende Bewertung, für welche Sicherheitsbehörden die Online-Durchsuchung in Betracht kommt, ist ebenfalls nicht zu finden. Die Online-Durchsuchung ist aber aufgrund ihrer technischen Eigenheiten nicht ohne Weiteres für alle Sicherheitsbehörden geeignet:¹³ Derzeit ist nicht ersichtlich, auf welchem technischen Weg der Herkunftsbeweis

und die Echtheitsbestätigung sichergestellt werden können. Diese benötigen Strafverfolgungsbehörden, wenn sie die erlangten Daten revisionsfest als Beweis verwenden wollen.¹⁴ Die Nachrichtendienste beschaffen in ihrem Aufgabenbereich vor allem Informationen über Bedrohungssituationen. Sie verfügen nicht über Befugnisse,



Gefahren abzuwehren. Dementsprechend führen die Beschwerdeführer einer neuen Verfassungsbeschwerde gegen die Befugnis zur Online-Durchsuchung, diesmal im Verfassungsschutzgesetz des Landes Bayern, an: Es sei nicht zielführend, einer Behörde einen Grundrechtseingriff zu gestatten, der mit einer Gefahr begründet wird, die diese Behörde gar nicht abwehren könne.¹⁵

Probleme bereitet außerdem die Zuständigkeitsverteilung bei der Terrorabwehr: Mit der Föderalismusreform 2006 war die Aufgabe der Abwehr des internationalen Terrorismus im Grundgesetz dem Bundeskriminalamt (BKA) zugewiesen worden.¹⁶ Dem BKA müssen deshalb mit einem Gesetz

Befugnisse eingeräumt werden, diese Aufgabe wahrnehmen zu können. Rechtsexperten kritisierten Mitte September bei der Anhörung im Innenausschuss, dass das jetzt vorgesehene BKA-Gesetz keine ausreichend klare Definition für den internationalen Terrorismus enthalte und somit unklar sei, wann das BKA zuständig wäre und in welchen Fällen weiterhin die Landespolizeien.¹⁷

Das alles hindert die Politik nicht daran, weiterhin lautstark und für alle Sicherheitsbehörden die Online-Durchsuchung zu fordern. Auf Bundesebene wird am BKA-Gesetz gearbeitet. Mehrere Bundesländer überarbeiten ihre Polizei- und Verfassungsschutzgesetze oder haben das wie Bayern schon getan. Inzwischen fordert auch das Bundesamt für Verfassungsschutz eine Befugnis zur Online-Durchsuchung.¹⁸ Auf Bundesebene wird am BKA-Gesetz gearbeitet. Der Bundestag hat bereits zugestimmt. Allerdings scheiterte das Gesetz zunächst an der Zustimmung der Länder im Bundesrat.¹⁹ Nachdem die Bundesregierung hiernach den Vermittlungsausschuss anrufen wollte, konnten sich CDU und SPD doch noch auf einen Kompromiss einigen: Der Kompromiss sieht vor allem vor, dass sowohl für die Anordnung der Online-Durchsuchung als auch bei der ersten Sichtung der gewonnenen Daten ein Richter zuständig sein soll. Der Kompromiss sieht allerdings keine Änderung für die differenzierte Behandlung von sogenannten Berufsgeheimnisträgern, also auch Journalisten, vor.²⁰ Es ist damit zu rechnen, dass das BKAG nun doch zum 1.1.2009 in Kraft treten wird.

Pressegeheimnisschutz und Online-Durchsuchung

Journalisten sind durch die Zulässigkeit einer Online-Durchsuchung in mehrfacher Hinsicht gefährdet. Journalisten wird in der Strafprozessordnung auch ein Zeugnisverweigerungsrecht wie anderen Berufsgeheimnisträgern eingeräumt. Während aber im Verhältnis zu Arzt oder Geistlichem regelmäßig die Vertraulichkeit des Kernbereichs privater Lebensgestaltung anzunehmen sein wird, gilt dies für den Journalisten im Verhältnis zu seinem Informanten nicht. Für den Journalisten ist somit schon von vornherein der absolute Grundrechtsschutz nicht gewährt, den die Garantie der Menschenwürde bietet. Es bleibt die durch

Journalisten sind durch die Zulässigkeit einer Online-Durchsuchung in mehrfacher Hinsicht gefährdet.

das Bundesverfassungsgericht abgeleitete Gewährleistung des Informantenschutzes aus der Pressefreiheit.²¹

das Bundesverfassungsgericht abgeleitete Gewährleistung des Informantenschutzes aus der Pressefreiheit.²¹

Im sogenannten Schäfer-Bericht²² wurde festgestellt, dass die gegen den Journalisten Schmidt-Engboom vorgenommenen Überwachungsmaßnahmen rechtswidrig waren. Das hinderte den Bundesnachrichtendienst (BND) nicht daran, kurz darauf auch den E-Mail-Verkehr einer Journalistin mit dem afghanischen Handelsminister zu überwachen.²³ Das Bundesverfassungsgericht stellte die Verfassungswidrigkeit der Vorgänge im Falle Cicero fest, da es immer nur darum gegangen sei, die Lecks im BKA selbst herauszufinden.²⁴ Dennoch wurden im Sommer 2007 Ermittlungsverfahren gegen Presseangehörige eingeleitet, die interne Informationen im Untersuchungsausschuss zum Fall Kurnaz veröffentlicht hatten, mit dem Ziel, die Person festzustellen, die die Informationen an die Presse herausgegeben hatte.²⁵

Das zeigt deutlich, dass weder Informanten- und Pressegeheimnisschutz noch die höchstrichterliche Rechtsprechung Gewähr dafür bieten, dass Ermittlungsbehörden die grundgesetzlich gebotene Rücksicht auf die Pressefreiheit nehmen.

Die verfassungsrichterliche Beurteilung solcher Fälle hindert die Ermittlungsbehörden nicht, Ermittlungsmaßnahmen durchzuführen, an denen freie Presse und Medien beteiligt sind. Dies wird durch einen Pressegeheimnisschutz in der Strafprozessordnung gefördert, der mit der



grundgesetzlichen Gewährleistung des Informantenschutzes nicht deckungsgleich ist.²⁶ Im Vordergrund steht hierbei zum einen, dass auch durch die Cicero-Entscheidung des Bundesverfassungsgerichts das Problem der sukzessiven Beihilfe zum Geheimnisverrat nicht aufgelöst wurde. Damit können die Ermittlungsbehörden weiterhin den Pressegeheimnisschutz aushebeln, indem sie Journalisten zu Beschuldigten machen.²⁷ Zum anderen ergibt sich für die Ermittler ein rechtmäßiges Zugriffspotenzial auf Journalisten durch die Unterscheidung zwischen Fremd- und Eigenmaterial. Während Letzteres dem aus dem Zeugnisverweigerungsrecht resultierenden Beschlagnahmeverbot unterliegt, ist Ersteres beschlagnahmefähig.²⁸ Wie wenig der Richtervorbehalt die Pressefreiheit wahrt, hat der Fall Cicero augenscheinlich unter Beweis gestellt.

Die Online-Durchsuchung verstärkt diese Defizite im Informantenschutz. Die Heimlichkeit der Online-Durchsuchung verhindert, dass Journalisten, die Ziel oder mitbetroffene Kontaktpersonen einer Online-Durchsuchung sind, wissen, dass sie ins Visier der Ermittlungsbehörden geraten sind. Sie können sich zwangsläufig nicht auf die Pressefreiheit berufen.

Nach dem momentan diskutierten Gesetzentwurf zum BKA-Gesetz (BKAG) wird der ohnehin vergleichsweise lückenhafte Pressegeheimnisschutz der Strafprozessordnung zusätzlich abgeschwächt.

Für Abgeordnete, Strafverteidiger und Geistliche – nicht solche islamischen Glaubens – ist auch im zukünftigen BKAG ein der Strafprozessordnung entsprechender Schutz vorgesehen.²⁹

Für sonstige Rechtsanwälte, Ärzte und Journalisten wird der Berufsgeheimnisträgerschutz im Vergleich zur Strafprozessordnung deutlich abgeschwächt, indem man ihn in das Ermessen des BKA stellt.

Zum Verhältnis zwischen dem Journalisten und seinem Informanten heißt es lapidar: „... ist dies im Rahmen der Prüfung der Verhältnismäßigkeit unter Würdigung des öffentlichen Interesses an den von dieser Person wahrgenommenen Aufgaben und des Interesses an der Geheimhaltung der

dieser Person anvertrauten oder bekannt gewordenen Tatsachen besonders zu berücksichtigen“.³⁰

Damit ist dem BKA auferlegt, die grundrechtliche Erwägung und Abwägung zwischen der Pressefreiheit und dem Abwehrinteresse des Staates zu ziehen. Eine angemessene Berücksichtigung der Belange von Informantenschutz und Pressefreiheit ist in das freie Ermessen der handelnden Behörde gestellt.

Die Online-Durchsuchung verstärkt diese Defizite im Informantenschutz.

Moralisch könnte dem Journalisten, der mit Verdächtigen zu tun hat, Terroristen sogar

unterstützt oder Bekennerschreiben um einer Reportage willen den Behörden vorenthält, die „Schutzwürdigkeit“ abgesprochen werden, stünde es außer Frage, dass die Online-Durchsuchung nur und ausschließlich als ultima ratio bei tatsächlichen Anhaltspunkten für terroristische Umtriebe und einer verstärkten Bedrohungslage eingesetzt würde.

Es gibt aber das Zeugnisverweigerungsrecht von Presseangehörigen und ein Beschlagnahmeverbot. Das Gesetz verlangt die Genehmigung einer Durchsuchung durch den Richter. Die Rechtsprechung des Bundesverfassungsgerichts zur Pressefreiheit räumt der freien Presse eine besondere Stellung und Bedeutung in der Demokratie ein. Dennoch geraten Journalisten nach wie vor und immer wieder in das Visier der Sicherheitsbehörden.

Das lässt nicht darauf vertrauen, dass Informantenschutz und Pressegeheimnisschutz im Entscheidungsspektrum der Ermittlungsbehörden manifestierte und selbstverständliche Rücksichtnahme hervorrufen.

Der BKA-Gesetzentwurf bestätigt außerdem eine schon länger abzusehende Entwicklung:³¹ Das BKAG hält den Wesensgehalt der Grundrechte ein. Es schreibt den vom Bundesverfassungsgericht verlangten Kernbereichsschutz vor. Es bewegt sich aber auch – bezogen auf alle dort vorgesehenen Befugnisse – an der von den Verfassungshütern festgelegten Grenze der Verfassungsmäßigkeit. Grundrechtsschutz wird nur noch soweit gewährleistet, wie dieser eingehalten werden muss. Die Balance zwischen Freiheit und Sicherheit ist nicht mehr zweifelsfrei gegeben. Die Sicherheit und das

Exklusiv für Journalisten:



+ 50 Cent für jeden Einkauf!

Die Kreditkarte mit vielen Extras!

**Sie legen als Journalist Wert auf Individualität und Details?
Zeigen Sie es mit der JournalistenCard und profitieren Sie!**

- 50 Cent Sofortbonus für jeden Einkauf ab 20 Euro
- 45 Tage Einkaufsversicherung
- Kreditrahmen unabhängig vom Girokonto
- Nur 10 Euro Jahresgebühr

Jetzt direkt beantragen:

0180 2 / 24 40 24

(Festnetz der Dt. Telekom – 0,06 Euro pro Anruf, ggf. abweichende Mobiltarife)

Die neue Generation Bank

ING  **DiBa**



Gegen die Infiltration	Maßnahme	Wirkung / Abwehr
Grundregeln	Es werden keine E-Mail-Anhänge oder Datenträger unbekannter Herkunft geöffnet bzw. installiert	Aktive Gegenwehr gegen beide vorgesehenen Infiltrationsmethoden => keine Infiltration möglich
	Der Rechner sollte nicht in der Grund- bzw. Hersteller-Konfiguration verbleiben	Die Infiltration ist mit einer standardisierten Software nicht möglich => Sonderanfertigung erforderlich
Weitergehende Sicherheitsmaßnahmen	Verwendung alternativer Betriebssysteme (z. B. Linux oder Mac) jenseits der Grundeinstellung	Die geringe Verbreitung und die Variabilität dieser Betriebssysteme erfordern eine überproportionale Maßarbeit bei der Softwareentwicklung => unwahrscheinlich
Sollte die Infiltration dennoch stattgefunden haben		
	Datenspeicherung auf externen Medien und vollständige Löschung auf dem Rechner	Die Daten sind auf dem Zielsystem nicht mehr verfügbar bzw. erzeugbar
	Asymmetrische Verschlüsselung sensibler Daten	Nur nach erheblichen Zeitaufwand – teilweise von Jahren – verwertbare Daten
Was weist auf eine Infiltration hin?		
	Das Hochladen von Datenpaketen in das Internet läuft wesentlich langsamer ab als ein Download. Da bei einer Online-Durchsuchung größere Datenmengen hochgeladen werden, verlangsamen sich alle mit dem Internet zusammenhängenden Tätigkeiten deutlich	Verlangsamen sich Browser, E-Mail-Programm, das Aufrufen von Websites und Up- und Downloads erheblich => Offline gehen
	Programme installieren, die Uploads aufzeichnen. Z. B. bei Linux im System vorgesehen.	

Bemühen darum sind in den Vordergrund getreten und verdrängen den Grundrechtsschutz als notwendiges Übel. Das gilt auch für die Pressefreiheit. Die Online-Durchsuchung oder auch der „große Lauschangriff“³² stellen Indizien für eine so geartete Tendenz dar.

Selbstschutzmaßnahmen

Im Gegensatz zu anderen Ermittlungsmaßnahmen bietet die Online-Durchsuchung in den vorgesehenen Varianten der Infiltrationen, ohne dass die Ermittler die Wohnung des Verdächtigen betreten müssten, einen nicht zu unterschätzenden Vorteil: Jeder kann sich hiervor ohne erheblichen Aufwand schützen.³³ Die Ermittler müssten alles über den verwendeten Computer wissen, um den Zugriff erfolgreich vornehmen zu können. Sensible Daten können außerdem von vornherein für eine Online-Durchsuchung unerschließbar gemacht werden. Sollte den Ermittlern aber dennoch das

Glück beschert sein, den „Bundestrojaner“ zu installieren, ist bei hinreichender Sensibilisierung der Zugriff zu erkennen und damit zu stören oder zu verhindern.

Werden die Grundregeln eingehalten, ist derzeit mit einer Infiltration nicht zu rechnen. Um auszuschließen, dass eigene Kommunikation mit einem Informanten registrierbar oder lesbar ist, wenn dessen Rechner Ziel einer Online-Durchsuchung sein sollte, ist neben allen eigenen Schutzmaßnahmen eine wirksame Verschlüsselung des E-Mail-Verkehrs und der Internettelefonie mit TrueCrypt³⁴, GnuPG³⁵ oder ähnlichen Produkten sinnvoll.

Die Online-Durchsuchung bleibt, was sie ist: Eine theoretisch einsetzbare Wunderwaffe, die in der praktischen Anwendung viele Hürden nehmen müsste. Die dementsprechend mehr hypothetische



Auseinandersetzung zeigt aber deutlich, dass die Innenminister, die Regierungen und die Gesetzgeber des Bundes und der Länder gewillt sind, für eine vermeintlich sicherere Zukunft die Grundrechte der Bürger einzuschränken. Für Presse und Medien gilt hier nichts anderes. Wahrscheinlich sind sie sogar gefährdeter als der Bürger, da die Medien häufig über Informationen verfügen, die auch die Sicherheitsbehörden gerne hätten.

- 32 BVerfG 1 BvR 2378/98 1 BvR 1084/99 v. 3.3.2004, http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html
 33 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 222
 34 <http://www.truecrypt.org/>
 35 <http://www.gnupg.org/>

Endnoten

- 1 <http://www.tagesschau.de/inland/meldung492374.html>
- 2 Ramelsberger in Süddeutsche Zeitung, 7.12.2006 Durchsuchung online Bei konkretem Tatverdacht hat die Polizei Zugriff auf die PCs der Bürger – das soll nun auch das BKA dürfen. <http://www.sueddeutsche.de/computer/artikel/965/93872/>
- 3 Burkhard Schröder in Die Online-Durchsuchung, Burkhard und Claudia Schröder, Heidelberg 2008, S. 43
- 4 ders. S. 42
- 5 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008 http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html, 1. Leitsatz
- 6 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 187
- 7 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 184
- 8 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, 2. Leitsatz
- 9 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, 3. Leitsatz u. Rn. 259
- 10 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 270 ff.
- 11 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 193
- 12 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 240
- 13 BVerfG 1 BvR 370/07 1 BvR 595/07 v. 27.2.2008, Rn. 254, vgl. auch Claudia Schröder, Wie die Vorgaben aus Karlsruhe die Phantasie beflügeln, telepolis 2.10.2008, <http://www.heise.de/tp/r4/artikel/28/28846/1.html>
- 14 Hansen, Pfitzmann, Roßnagel, Online-Durchsuchung DriZ 2007, 225 <http://www.heymanns.com/servlet/PB/menu/1226897/index.html>
- 15 Will, Klageschrift von Mitgliedern der bayerischen SPD-Landtagsfraktion v. 18.9.2008, S. 40, http://bayernspd.de/work-space/uploads/pdfs/VB_final_Schriftsatzvom18.9.2008_o.U._o.A..pdf
- 16 http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/index.html
- 17 http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung15/Stellungnahmen_SV/index.html, v.a. Kutscha, Geiger, Gusy und Poscher (S. 19)
- 18 <http://www.heise.de/newsticker/Verfassungsschutz-beharrt-auf-heimlichen-Online-Durchsuchungen--/meldung/120110>
- 19 <http://www.heise.de/newsticker/Keine-Mehrheit-im-Bundesrat-fuer-das-BKA-Gesetz--/meldung/119581>
- 20 <http://www.heise.de/newsticker/SPD-und-Union-einigen-sich-beim-BKA-Gesetz-Update--/meldung/119791>
- 21 BVerfGE 66,116 (133 ff.); 107,299 (331), 20,162 (191 f., 217)
- 22 http://www2.bundestag.de/bnd_bericht.pdf
- 23 <http://www.zeit.de/online/2008/17/bnd-uhrlau-pkg>
- 24 BVerfG 1 BvR 538/06 v. 27.2.2007, http://www.bundesverfassungsgericht.de/entscheidungen/rs20070227_1bvr053806.html
- 25 <http://www.tagesschau.de/inland/meldung6506.html>
- 26 Dunkhase, Das Pressegeheimnis, Berlin 1998, S. 83 f.
- 27 ders., S. 97 f.
- 28 ders., S. 104 f.
- 29 E-BKAG, § 20 u Absatz 1
- 30 E-BKAG, § 20 u Absatz 2 u. 3
- 31 Vgl. Lepsius, Das Verhältnis von Sicherheit und Freiheitsrechten in der Bundesrepublik Deutschland nach dem 11. September 2001, <http://www.aicgs.org/documents/lepius.pdf>

Die Autorin:

Claudia Schröder studiert Rechtswissenschaften an der Europauniversität Viadrina in Frankfurt/Oder mit dem Studienschwerpunkt Medienrecht. Sie hat sich seit ihrem Wiedereinstieg in das Jurastudium wissenschaftlich und publizistisch umfangreich mit Rechtsfragen im Spannungsfeld zwischen politischen Sicherheitsbestrebungen und neuen Medien befasst. Im September 2008 erschien das Buch „Die Online-Durchsuchung“, dessen juristische Abhandlung sie als Co-Autorin verfasste.

