DuD
Datenschutz und Datensicherheit

Ermächtigungsgrundlage für die „Online-Durchsuchung“?

Verfassungsrechtliche Anforderungen an und Grenzen für den heimlichen Zugriff auf IT-Systeme im Ermittlungsverfahren

Gerrit Hornung

Ende Januar 2007 hat der 3. Strafsenat des Bundesgerichtshofs (BGH) entschieden, dass die „verdeckte Online-Durchsuchung“ im Strafprozess mangels gesetzlicher Ermächtigungsgrundlage unzulässig ist. Seitdem wird vielfach die Einführung einer derartigen Norm gefordert. Die Analyse de lege ferenda zeigt, dass die erforderliche Beachtung der neueren verfassungsgerichtlichen Rechtsprechung zum Kernbereich des Persönlichkeitsrechts den Gesetzgeber vor erhebliche Probleme stellen wird. Überdies sperrt Art. 13 GG gegenwärtig die Verabschiedung einer einfachgesetzlichen Ermächtigungsgrundlage. Schließlich ergeben sich wichtige praktische Probleme, für die bislang keine Lösungen erkennbar sind.

Dr. *Gerrit Hornung*, LL.M.

Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) und wissenschaftlicher Mitarbeiter an der Universität Kassel
E-Mail: gerrit.hornung@uni-kassel.de

1 Einleitung

Die so genannte Online-Durchsuchung hat seit dem 25. November 2006 eine bemerkenswerte Karriere in der öffentlichen Diskussion gemacht.[1] An diesem Tag lehnte es der Ermittlungsrichter des BGH ab, auf einen Antrag der Bundesanwaltschaft *„gemäß §§ 102, 105 Abs. 1, 94, 98, 169 Abs. 1 Satz 2 StPO die Durchsuchung des von dem Beschuldigten […] benutzen Personalcomputers/Laptops, insbesondere der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien…, und deren Beschlagnahme anzuordnen und […] zur verdeckten Ausführung dieser Maßnahme zu gestatten, ein hierfür konzipiertes Computerprogramm dem Beschuldigten zur Installation zuzuspielen, um die auf den Speichermedien des Computers abgelegten Dateien zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen“*.[2]

Nach der Bestätigung durch den 3. Strafsenat des BGH[3] begann eine Debatte um die Einrichtung einer Ermächtigungsgrundlage. Eine solche findet sich bislang nur in § 5 Abs. 2 Nr. 11 VSG NRW; insoweit ist eine Verfassungsbeschwerde anhängig.[4] In der Schweiz soll der neue § 18 m des Gesetzes über Maßnahmen zur Wahrung der inneren Sicherheit eine ähnliche Norm enthalten.[5]

2 Begriff und Technik

Der Begriff der „Online-Durchsuchung“ weist eine große Unschärfe hinsichtlich der technischen Abläufe auf. Der BGH verwendet ihn als Synonym für die beantragte, oben zitierte Maßnahme. In (mindestens) zwei Punkten stellt diese jedoch nur einen Ausschnitt der Problematik dar, nämlich hinsichtlich des Angriffsobjekts (PC / Laptop) und der Angriffsmethode (Installation eines Computerprogramms). „Online-Durchsuchung“ sollte deshalb als Sammelbezeichnung für das der Intention nach für den Nutzer unmerkliche Ausspähen und/oder Kopieren der in einem IT-System gespeicherten Daten durch staatliche Behörden über einen Internetzugang verstanden werden.[6]

Dieser Angriff muss nicht zwingend über eine Online-Verbindung (sei es als E-Mail-Anhang oder Verborgen in einem Download des Nutzers)[7] beginnen, wie dies durch die Bezeichnung „Bundes-Trojaner“ suggeriert wird. Die Software kann dem Adressaten auch über eine CD mit vorgeblich interessanten Inhalten zugespielt oder sogar durch Ermittlungsbeamte direkt im System installiert werden, so diese physischen Zugriff

[1] S. zuvor *Bär*, MMR 1998, 463 ff.; *Germann*, Gefahrenabwehr und Strafverfolgung im Internet, 2000, 540 ff.; *Zöller*, GA 2000, 562, 568 ff.; *Böckenförde*, Die Ermittlung im Netz, 2003, 209 ff.; *Hofmann*, NStZ 2005, 121 ff.

[2] BGH, DuD 2007, 134, (am 28.11.2006 auf die Beschwerde der Generalbundesanwältin bestätigt) s. *Hornung*, CR 2007, 144; *Bär*, MMR 2007, 175; *Jahn/Kudlich*, JR 2007, 57.

[3] BGH, NJW 2007, 930; s. *Hamm*, NJW 2007, 932; *Bär*, MMR 2007, 239; *Schaar/Landwehr*, K&R 2007, 202; *Harrendorf*, StraFo 2007, 149.

[4] Verfasst vom Berliner Anwalt *Roggan*; s. http://www.heise.de/tp/r4/artikel/24/24727/1.htm.

[5] Zu den Regierungsplänen http://www.heise.de/newsticker/meldung/91247.

[6] Zu den Möglichkeiten z.B. *Schmidt*, http://www.heise.de/security/artikel/86415/; *Buermeyer*, HRRS 2007, 154 ff.

[7] S. dazu *Buermeyer*, HRRS 2007, 154, 163 f.

haben.[8] In jedem Fall wird allerdings eine Online-Verbindung zum Übermitteln der Daten an die Behörden benötigt.

Über technische Einzelheiten der offenbar bereits erfolgten und künftig geplanten Online-Durchsuchungen gibt es keine öffentlichen Informationen.[9] In den USA wurden offenbar Versuche mit verschiedenen Angriffsformen unternommen („Magic Lantern“ und andere).[10] Der Antrag der Bundesanwaltschaft, „ein hierfür konzipiertes Computerprogramm dem Beschuldigten zur Installation zuzuspielen“ (s.o.), könnte sich sowohl auf einen E-Mail-Anhang, als auch auf die Variante des Verschickens einer CD beziehen. Die Bundesregierung hat lediglich erklärt, der einmalige Investitionsaufwand für die Maßnahme betrage etwa 200.000 Euro; es seien zwei zusätzliche Programmierer erforderlich.[11] Die Unkenntnis über den genauen technischen Ablauf erschwert nicht nur die politische Diskussion, sondern auch die verfassungsrechtliche Analyse in erheblichem Umfang.

An dieser Stelle kann nicht erörtert werden, inwieweit Trojaner oder andere Angriffsformen tatsächlich erfolgversprechend zum Ziel der hoheitlichen Informationsbeschaffung eingesetzt werden können. Jedenfalls gibt es deutlich skeptische Stimmen hinsichtlich der derzeitigen Fähigkeiten der Sicherheitsbehörden.[12] Diese beziehen sich vor allem auf die technischen Grenzen der Übertragung großer Datenmengen (im Upstream) und die Fähigkeit von Kriminellen, ihre Systeme durch Verwendung sicherer Betriebssysteme, Firewalls, Antivirenprogramme, Verschlüsselungssoftware und andere Mechanismen wirksam abzuschotten.

Nach einem erfolgreichen Angriff, dessen Möglichkeit – auch angesichts der Antragstellung der Bundesanwaltschaft – für die rechtliche Analyse unterstellt werden soll, hätte die ermittelnde Behörde weitreichende Zugriffsmöglichkeiten auf das System. Denkbar wäre das (je nach Speicherumfang und Verbindungsgeschwindigkeit teilweise oder vollständige) Kopieren des Festplatteninhalts, das Mitschneiden der Kommunikation in drahtgebundenen und drahtlosen Intranets und im Internet (E-Mail, Datenfernübertragung, Internettelefonie) und das Aktivieren angeschlossener Mikrofone und Webcams.[13] Außerdem bestehen – ohne diesbezüglich Unterstellungen machen zu wollen – die Möglichkeiten, Daten zu löschen, hinzuzufügen und zu manipulieren sowie das System insgesamt abzuschalten und ganz oder teilweise zu blockieren.[14]

3 Keine StPO-Grundlage

Die einzige ausdrückliche Ermächtigungsgrundlage für eine Online-Durchsuchung findet sich in § 5 Abs. 2 Nr. 11 VSG NRW. Dagegen ist umstritten, ob die Maßnahme direkt oder analog auf § 102 StPO gestützt werden kann.[15] Im Februar 2006 hatte zunächst ein Ermittlungsrichter des BGH eine Online-Durchsuchung auf dieser Basis genehmigt,[16] Ende November desselben Jahres ein anderer Ermittlungsrichter einen entsprechenden Antrag abgelehnt und schließlich der 3. Strafsenat desselben Gerichts die hiergegen erhobene Beschwerde der Bundesanwaltschaft verworfen.[17]

Die letztgenannten Entscheidungen sind überzeugend. Das Gericht lehnt die Anwendung von § 102 StPO mit dem entscheidenden Argument ab, die in §§ 105 Abs. 2, 106 f. StPO normierte Offenheit der gesetzlich vorgesehenen Durchsuchung sei hier per definitionem ausgeschlossen.[18] Diese Auslegung des Durchsuchungsbegriffs ist nicht etwa „dogmatisch bereits im Ansatz nicht haltbar“,[19] sondern im Rahmen der systematischen Auslegung geboten. Der BGH stellt zu Recht fest, dass es sich bei den Regelungen um zwingendes Recht handelt. Außerdem rechtfertige die Tatsache, dass Verstöße nach herrschender Ansicht jedenfalls nicht immer zu einem Beweisverwertungsverbot führen, nicht den Schluss, die Behörden dürften Maßnahmen ergreifen, die schon ihrer Natur nach wesentliche Verfahrensvorschriften verletzen.

Andere Eingriffsnormen decken die Maßnahme nicht. § 100 a StPO ist nicht einschlägig: Die Ausforschung des Systeminhalts erfolgt zwar mittels Telekommunikation, ist aber nicht selbst deren Überwachung.[20] § 100 c StPO greift nicht, weil es nicht um das in einer Wohnung nichtöffentlich gesprochene Wort geht; § 100 f Abs. 1 Nr. 2 StPO gestattet nur den Einsatz technischer Mittel außerhalb von Wohnungen; die Generalklausel in § 161 StPO deckt nur Maßnahmen, die lediglich geringfügige Grundrechtseingriffe mit sich bringen.[21]

4 Zulässigkeit de lege ferenda

Die Frage der Ermächtigungsgrundlage im geltenden Recht ist damit zumindest für die Praxis negativ beantwortet. Vor dem Hintergrund der politischen Forderungen nach einer Gesetzesänderung stellt sich die Frage der verfassungsrechtlichen Zulässigkeit. Die Online-Durchsuchung kann den Schutzbereich mehrerer Grundrechte der Beschuldigten – und eventuell der sonstigen Nutzungsberechtigten der IT-Systeme – berühren.

4.1 Kernbereich privater Lebensgestaltung

Art. 1 Abs. 1 GG gewährt einen *„unantastbaren Kernbereich privater Lebensgestaltung“*.[22] In diesem findet keine Abwägung zwischen den Grundrechten des Einzelnen und den öffentlichen Gefahrenabwehr- und

[8] S. http://www.dradio.de/dlf/sendungen/computer/620126/.

[9] S.a. *Gercke*, CR 2007, 245, 246; die Bundesregierung erklärte im April 2007, die Ausgestaltung der Maßnahme werde noch geprüft, s. BT-Drs. 16/4997, 2.

[10] S. http://www.heise.de/tp/r4/artikel/11/11333/1.html.

[11] BT-Drs. 16/3973, 4.

[12] Z.B. *Kutscha*, NJW 2007, 1169, 1171 f.; *Gercke*, CR 2007, 245, 248 f.; *Buermeyer*, HRRS 2007, 154, 164 f.; *Kling*, http://www.heise.de/tp/r4/artikel/24/24678/1.html; *Schröder*, http://www.heise.de/tp/r4/artikel/24/24587/1.html (mit lesenswerter Analyse der Entstehungsgeschichte der Meldungen in den Medien).

[13] S. näher *Buermeyer*, HRRS 2007, 154, 159 ff.; s.a. *Gercke*, CR 2007, 245, 246 ff.

[14] S. *Harrendorf*, StraFo 2007, 149, 150 f.; *Schaar/Landwehr*, K&R 2007, 202, 205.

[15] Dafür v.a. *Graf*, DRiZ 1999, 281, 285; *Hofmann*, NStZ 2005, 121, 123 ff. m.w.N.

[16] BGH, StV 2007, 60 mit abl. Anm. *Beulke/Meininghaus*; s.a. *Störing*, c't 5/2007, 58, 59.

[17] S.o. 1.

[18] Ebenso *Bär*, MMR 1998, 463, 466 ff.; *ders*., MMR 2007, 175 f.; *Zöller*, GA 2000, 563, 572 f.; *Germann* (Fn. 1), 544; *Böckenförde* (Fn. 1), 214 ff.; *Jahn/Kudlich*, JR 2007, 57, 58 ff.; *Beulke/Meininghaus*, StV 2007, 63, 64 f.; *Rux*, JZ 2007, 285, 290 f.; *Hornung*, CR 2007, 144; *Gercke*, CR 2007, 245, 250 f.; *Kemper*, ZRP 2007, 105, 106 f.; s.a. *Schäfer* in: Löwe/Rosenberg, StPO, 25. Aufl. 2003, § 106 Rn. 1.

[19] So aber *Hofmann*, NStZ 2005, 121, 124.

[20] BGH, NJW 2007, 930, 931 f.; ebenso schon *Bär*, MMR 1998, 463, 467; *ders.*, MMR 2007, 175, 176 f.; *Germann* (Fn. 1), 543 f.; *Zöller*, GA 2000, 563, 573 f.; *Jahn/Kudlich*, JR 2007, 57, 60 f.; ähnlich *Hofmann*, NStZ 2005, 121, 122 f.

[21] *Meyer-Goßner*, StPO, 49. Aufl. 2006, § 161 Rn. 1.

[22] S. v.a. BVerfGE 109, 279 (311 ff.); ferner BVerfGE 6, 32 (41); 27, 1 (6); 80, 367 (373).

Strafverfolgungsinteressen statt.[23] Als Kriterien für die Betroffenheit des Kernbereichs nennt das Gericht etwa den Bezug zu Art. 13 GG und die Äußerungen innerster Gefühle oder von Ausdrucksformen der Sexualität. Gleichzeitig betont es, dass *„Aufzeichnungen oder Äußerungen im Zwiegespräch, die zum Beispiel ausschließlich innere Eindrücke und Gefühle wiedergeben und keine Hinweise auf konkrete Straftaten enthalten, […] nicht schon dadurch einen Gemeinschaftsbezug [gewinnen], dass sie Ursachen oder Beweggründe eines strafbaren Verhaltens freizulegen vermögen"*.[24]

Je nach Inhalt des durchsuchten Systems kann dieser Kernbereich privater Lebensgestaltung berührt sein. Auf privaten und betrieblichen Rechnern werden heute elektronische Steuerdaten (für das ELSTER-Verfahren), Kontoführungsinformationen, elektronische Rechnungen, Betriebs- und Geschäftsgeheimnisse, Gesundheitsinformationen (Korrespondenz, Befunde, künftig auch Daten der elektronischen Gesundheitskarte), Einzelverbindungsnachweise über Telekommunikationsvorgänge, E-Mails, Adressdaten, wissenschaftliche Texte, private Fotos, Videos, intime Briefe und Tagebücher gespeichert – die Liste ließe sich fortsetzen –, und Mikrofone und Webcams an sie angeschlossen.[25] Insbesondere Briefe, elektronische Tagebücher, Bilder und Filme sowie Gesundheitsinformationen werden leicht in den Kernbereich fallen. Überdies zeigen die Beispiele der angeschlossenen Mikrofone und Webcams, dass in bestimmten Fällen kein Unterschied zur akustischen Wohnraumüberwachung besteht.

Bestehen Anhaltspunkte für eine Verletzung der Menschenwürde, so muss die Überwachung von vornherein unterbleiben.[26] Werden unerwartet absolut geschützte Informationen erhoben, ist die Überwachung abzubrechen und sind die Aufzeichnungen zu löschen; jede Verwendung der Daten ist ausgeschlossen. Diese Anforderungen müssten für die Online-Durchsuchung in einem Gesetz geregelt werden.[27] Dies gilt auch für die Tätigkeit der Verfassungsschutzbehörden.[28] Bereits daraus folgt, dass die gegenwärtige Regelung in § 5 Abs. 2 Nr. 11 VSG NRW, die diese Anforderungen nicht erfüllt, mit Art. 1 Abs. 1 GG nicht vereinbar ist.[29]

Die Beachtung der verfassungsrechtlichen Anforderungen dürfte in der Praxis erhebliche Probleme bereiten, weil im Regelfall erst nach Kenntnisnahme des Inhalts gespeicherter Daten beurteilt werden kann, ob sie zum Kernbereich gehören, das BVerfG jedoch ausdrücklich festgestellt hat, dass es unzulässig ist, zum Zwecke der Feststellung der Betroffenheit des Kernbereichs in diesen einzugreifen.[30] Eine praktikable Lösung für dieses Problem ist bislang kaum erkennbar.[31] Denkbar wäre zwar ein Schutz durch erweiterte Beweisverwertungsverbote oder eine zusätzliche richterliche Kontrolle des Materials vor seiner Verwendung durch die Strafverfolgungsbehörden. Diese Variante – beim Lauschangriff „Richterband" genannt[32] – birgt aber die Gefahr, dass Unberechtigte auf das Material zugreifen. Überdies (und fundamentaler) dürfte in der Praxis kaum auszuschließen sein, dass das gewonnene Wissen nicht doch verwendet wird.[33]

Sollte es im Ergebnis nicht möglich sein, eine mit dem Kernbereichsschutz konforme Durchführung der Online-Durchsuchung vorzunehmen, so kann dies nicht zur Aufgabe dessen Schutzes führen. Vielmehr wäre die Maßnahme in diesem Fall insgesamt unzulässig.

4.2 Art. 13 GG

Von besonderer Bedeutung ist die Frage, ob die Online-Durchsuchung den Schutzbereich von Art. 13 Abs. 1 GG berührt. Das Grundrecht auf Unverletzlichkeit der Wohnung verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in ihm in Ruhe gelassen zu werden.[34] Geschützt wird also die „räumliche Privatsphäre";[35] historisch vor allem gegen Eingriffe durch physische Anwesenheit von Trägern öffentlicher Gewalt. Das BVerfG hat aber überzeugend dargelegt, dass unter den Bedingungen moderner Überwachungstechnologien *„der Schutzzweck der Grundrechtsnorm vereitelt [würde], wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel, auch wenn sie von außerhalb der Wohnung eingesetzt werden, nicht von der Gewährleistung […] umfasst wäre"*.[36]

Art. 13 Abs. 1 GG greift deshalb ein, wenn auf ein IT-System zugegriffen wird, welches sich im räumlichen Geltungsbereich[37] des Grundrechts befindet. Das dürfte jedenfalls dann kaum zu bestreiten sein, wenn das System nicht über eine Online-Verbindung verfügt und ein Zugriff durch technische Hilfsmittel anderer Art erfolgt (optisches Überwachen von Bildschirmen, Aufzeichnung der Abstrahlung von Computermonitoren oder Ähnliches).[38]

Die entscheidende Frage ist folglich, ob der Schutz von Art. 13 Abs. 1 GG dadurch aufgehoben wird, dass der Nutzer des Systems dieses mit dem Internet verbindet. Zunächst ändert dies nichts daran, dass sich dieses mitsamt der auf ihm gespeicherten Daten in der „räumlichen Privatsphäre" des Nutzers befindet. Das Argument, durch die Online-Durchsuchung bleibe „der Raum, in welchem sich der Computer befindet, […] unangetastet",[39] verkennt, dass Art. 13 GG nicht diesen Raum um seiner selbst willen, sondern wegen der Privatsphäre schützt, in der der Einzelne sich ungestört verhalten können soll. Mit derselben Argumentation

[23] Vgl. näher z.B. *Denninger*, ZRP 2004, 101 ff.; *Kutscha*, NJW 2005, 20 ff.; *Löffelmann*, NJW 2005, 2033 ff.; *Lindemann*, JR 2006, 191 ff.; sowie die Beiträge in *Roggan* (Hrsg.), Lauschen im Rechtsstaat, 2004; *Schaar* (Hrsg.), Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung, 2005.

[24] BVerfGE 109, 279 (319).

[25] Dieser Bereich wird „in der modernen Gesellschaft vielfach als intimster und sicherster Rückzugsort für Informationen, Kommunikationen etc. empfunden" (*Jahn/Kudlich*, JR 2007, 57, 59); s.a. *Rux*, JZ 2007, 285, 291; *Kutscha*, NJW 2007, 1169, 1170 f.; *Harrendorf*, StraFo 2007, 149, 150 f. Deshalb ist es unzutreffend, dass der Kernbereich allenfalls am Rande tangiert sei, so *Bär*, MMR 2007, 239, 242.

[26] S. im Einzelnen BVerfGE 109, 279 (318).

[27] Entsprechend den Regelungen zur Wohnraumüberwachung in § 100c bis § 100e StPO.

[28] Der Kernbereichsschutz gilt hier identisch, s. SächsVerfGH, NVwZ 2005, 1310 ff.; *Perne*, DVBl. 2006, 1486, 1487; *Denninger*, ZRP 2004, 101, 104.

[29] Ebenso *Humanistische Union*, Stellungnahme 14/628 zur Änderung des VSG NRW, 11; *Roggan* (Fn. 4), unter C. III. 2. b).

[30] BVerfGE 109, 279 (323).

[31] *Kutscha*, NJW 2007, 1169, 1171; s. allgemein bereits *Petersen*, KJ 2004, 316, 324;

[32] Ausführlich *Perne*, DVBl. 2006, 1486 ff.

[33] S. die Nachweise in Fn. 31; ferner *Denninger* in: Roggan (Fn. 23), 18 f.

[34] BVerfGE 32, 54 (75); 42, 212 (219); 51, 97 (110); 109, 279 (309).

[35] BVerfGE 7, 230 (238); 109, 279 (309).

[36] BVerfGE 109, 279 (309).

[37] Dazu z.B. *Jarass* in: ders./Pieroth, GG, 8. A. 2006, Art. 13 Rn. 2 ff.; *Gornig* in: v. Mangoldt/Klein/Starck, GG, 5. A. 2005, Art. 13 Rn. 13 ff.; jeweils m.w.N.

[38] Mit diesem Ausgangspunkt auch *Roggan* (Fn. 4), unter C. III. 1.

[39] BGH (Ermittlungsrichter), StV 2007, 60, 62, ebenso *Graf*, DRiZ 1999, 281, 285; *Hofmann*, NStZ 2005, 121, 124.

könnte man behaupten, auch die akustische Wohnraumüberwachung ließe den Raum, in dem sich die kommunizierenden Menschen befinden, unangetastet. Art. 13 GG schützt aber gegen jede Kenntniserlangung von Geschehnissen innerhalb der Wohnung.[40]

Auch das Argument, die räumliche Abschottung des Rechnerstandortes sei für Online-Zugriffe ohne Belang,[41] trägt nicht. Dies würde perspektivisch dazu führen, dass alle Daten, die künftig durch Sensoren und „intelligente“ vernetzte Gegenstände in Wohnräumen erfasst werden, nicht mehr von Art. 13 GG erfasst wären, obwohl sie Aufschluss über private Lebensgewohnheiten in diesen Räumen geben. Ganz grundsätzlich ist die Reichweite des Schutzbereichs nicht aus der Perspektive der Behörden, sondern aus der des Grundrechtsträgers zu bestimmen. Es wäre geradezu widersinnig, diesem den Grundrechtsschutz gerade dort zu versagen, wo er neuen Ermittlungsmaßnahmen ausgesetzt ist, die technisch so ausgefeilt sind, dass die Mauern der Wohnung keinen Schutz bieten. Dies würde nicht nur den Schutzbereich vom technischen Fortschritt abhängig machen, sondern ihn auch kontinuierlich reduzieren.

In der Verbindung mit dem Internet liegt auch keine Einwilligung in den Zugriff auf das System.[42] Selbst wenn (etwa bei Filesharing-Systemen) eine Gestattung vorliegt, beschränkt sich der Zugriff auf vom Nutzer bestimmte, abgrenzbare Teile der Festplatte. Weitergehende Zugriffe stellen einen Missbrauch gegen den Willen des Nutzers dar und können nicht dazu führen, ihn seines Grundrechtsschutzes zu berauben.

Im Ergebnis ist Art. 13 Abs. 1 GG somit anwendbar, wenn sich das IT-System in der Wohnung oder einem sonstigen von der Norm geschützten Raum befindet.[43] Das führt allerdings zu praktischen Problemen, weil für die Behörden nicht erkennbar ist, ob sie auf ein mobiles Endgerät (z.B. ein Laptop) zugreifen, das sich gerade nicht im Schutzbereich befindet. Um dem zu entgehen, ist vorgeschlagen worden, Art. 13 GG im Wege der Analogie auf „virtuelle Räume“ (Datenspeicher) zu erweitern.[44] Dieser weitreichende Ansatz wirft grundsätzliche verfassungsdogmatische Probleme auf, die an dieser Stelle nicht erörtert werden können. Zutreffend ist aber jedenfalls, dass der beschriebene Konflikt nicht zulasten derjenigen Grundrechtsträger aufgelöst werden kann, die – da sich ihre IT-Systeme in dessen räumlichen Schutzbereich befinden – den Schutz von Art. 13 GG genießen.[45]

Eine Lösung wird erkennbar, wenn man Folgendes berücksichtigt: So die Behörden damit rechnen müssen, in ein Grundrecht einzugreifen, dies jedoch nicht genau wissen, müssen sie – zumindest solange es sich wie hier nicht um ganz fernliegende, atypische Einzelfälle handelt – die Anforderungen für einen solchen Eingriff einhalten, auch wenn dies im Einzelfall objektiv nicht erforderlich sein sollte. Das gilt auch für den Gesetzgeber bei der Schaffung einer gesetzlichen Ermächtigungsgrundlage für die Online-Durchsuchung, die sich folglich an Art. 13 GG messen lassen muss.

De lege lata bedeutet dies, dass die Maßnahme zu Strafverfolgungszwecken[46] nicht nur einfachgesetzlich, sondern auch verfassungsrechtlich unzulässig ist.[47] Sie kann nach den Schrankenregelungen von Art. 13 GG nicht gerechtfertigt werden.[48] Es handelt sich weder um ein technisches Mittel zur akustischen Überwachung (Art. 13 Abs. 3 GG), noch um Maßnahmen zur Gefahrenabwehr (Art. 13 Abs. 4 und 7 GG) oder zum Schutze eingesetzter Personen (Art. 13 Abs. 5 GG). Auch eine „Durchsuchung“ (Art. 13 Abs. 2 GG) liegt nicht vor. Die Argumente des BGH zu § 102 StPO[49] sind insoweit übertragbar. Art. 13 Abs. 2 GG geht zwar nicht explizit, wohl aber der Sache nach gleichfalls vom hergebrachten Bild der offenen Durchsuchung durch körperlich anwesende Personen aus.[50] Aus demselben Grund konnte vor der Änderung von Art. 13 GG die akustische Wohnraumüberwachung nicht als eine Art „akustische Durchsuchung“ gerechtfertigt werden.[51]

Im Ergebnis erfordert die Maßnahme eine Änderung des Grundgesetzes. Ob der Anlass diese tiefgreifende Maßnahme rechtfertigt, ist überaus zweifelhaft. Sollte der verfassungsändernde Gesetzgeber eine entsprechende Entscheidung fällen, wären jedenfalls auch bei der Grundgesetzänderung die Vorgaben des Kernbereichsschutzes[52] zu beachten.

4.3 Art. 10 Abs. 1 GG

Das Fernmeldegeheimnis ist betroffen, wenn durch die aufgespielte Software die aktuelle Kommunikation des Systems mit Dritten aufgezeichnet wird. Das ist jedoch nicht das Ziel der Online-Durchsuchung. Werden Daten vom Zielrechner kopiert, so ist Art. 10 Abs. 1 GG nicht einschlägig.[53] Das gilt auch für E-Mails oder andere empfangene Daten, weil nach dem Empfang keine Kommunikation mehr vorliegt; die

[40] *Cassardt* in: Umbach/Clemens, GG, Art. 13 Rn. 38 m.w.N.; *Kunig* in: v. Münch/Kunig, GG, 5. A. 2000, Art. 13 Rn. 17; s.a. *Gornig* (Fn. 37), Art. 13 Rn. 43.

[41] So *Germann* (Fn. 1), 540 ff.; *Böckenförde* (Fn. 1), 222 ff.; *Beulke/Meininghaus*, StV 2007, 63, 64; *Gercke*, CR 2007, 245, 250; ähnlich *Cassardt* (Fn. 40), Art. 13 Rn. 43.

[42] In diese Richtung *Hofmann*, NStZ 2005, 121, 124; *Bundesamt für Verfassungsschutz*, Stellungnahme 14/639 zur Änderung des VSG NRW, 6; *Kemper*, ZRP 2007, 105, 109; wie hier *Kutscha*, NJW 2007, 1169, 1170; *Harrendorf*, StraFo 2007, 149, 151 f.

[43] Ebenso *Jahn/Kudlich*, JR 2007, 57, 60; *Bär*, MMR 2007, 175, 176; *ders*., MMR 2007, 239, 240; *Kutscha*, NJW 2007, 1169 ff.; *Harrendorf*, StraFo 2007, 149, 152; *Schaar/Landwehr*, K&R 2007, 202, 204; *Huster*, Stellungnahme 14/641 zur Änderung des VSG NRW, 4; *Sokol*, ebd., Stellungnahme 14/625, 11 ff. ; a.A. *Gusy*, ebd., Stellungnahme 14/629, 6; *Cassardt* (Fn. 40), Art. 13 Rn. 43; *Beulke/Meininghaus*, StV 2007, 63 f.

[44] *Rux*, JZ 2007, 285, 292 ff.

[45] So aber *Beulke/Meininghaus*, StV 2007, 63, 64, die aus dem Postulat, „ein portables Internetgerät [werde] vor dem Online-Zugriff nicht besser oder schlechter geschützt, je nachdem ob sich Nutzer und Gerät im Freien oder in einer Wohnung befinden“, ableiten, der schlechtere Schutz sei auch im zweiten Fall angemessen.

[46] Zur Gefahrenabwehr wäre eine Rechtfertigung unter den Voraussetzungen von Art. 13 Abs. 4 GG (dringende Gefahr für die öffentliche Sicherheit, Beachtung des Richtervorbehalts) möglich, der z.B. auch Videokameras erfasst, s. z.B. *Gornig*, (Fn. 37), Art. 13 Rn. 129. Hierfür reichen aber die allgemeinen Generalklauseln der Gefahrenabwehrbehörden schon aufgrund des Wesentlichkeitsgrundsatzes nicht aus, s. *Rux*, JZ 2007, 285, 286 ff.; ebenso Begründung zum VSG NRW, LT-Ds. 14/2211, 17 f.; s.a. *Germann* (Fn. 1), 546; a.A. *Zöller*, GA 2000, 563, 576. Ermächtigungen für Verfassungsschutzbehörden sind unzulässig, soweit sie über Art. 13 Abs. 4 GG hinausgehen (*Baldus* in: Schaar (Fn. 23), 24 ff.). § 5 Abs. 2 Nr. 11 VSG NRW verletzt überdies das Erfordernis einer richterlichen Anordnung.

[47] S.a. *Jahn/Kudlich*, JR 2007, 57, 60; *Schaar/Landwehr*, K&R 2007, 202, 204 f.

[48] Das bleibt unerwähnt bei *Kutscha*, NJW 2007, 1169 ff.; *Harrendorf*, StraFo 2007, 149, die nur den Schutzbereich prüfen.

[49] S.o. 3.

[50] *Papier* in: Maunz/Dürig, GG, Art. 13 Rn. 47; *Cassardt* (Fn. 40), Art. 13 Rn. 68; *Kunig* (Fn. 40), Art. 13 Rn. 24 ff.; *Jahn/Kudlich*, JR 2007, 57, 59.

[51] Damals h.M., s. *Gornig* (Fn. 37), Art. 13 Abs. 2 Rn. 66; *Krey/Haubrich*, JR 1992, 309, 313; *Eisenberg*, NJW 1993, 1033, 1038; *Kutscha*, NJW 1994, 85, 87, jeweils m.w.N; s.a. *Ruthig*, JuS 1998, 506, 511 ff.

[52] S.o. 4.1.

[53] Wohl allg.M., s. z.B. BGH, StV 2007, 60, 62; *Rux*, JZ 2007, 285, 292; *Bär*, MMR 2007, 239, 240; *Beulke/Meininghaus*, StV 2007, 63, 64.

Daten werden durch das Recht auf informationelle Selbstbestimmung geschützt.[54]

4.4 Geheimnisschutz

Nur am Rande sei – aus aktuellem Anlass – darauf verwiesen, dass in speziellen Konstellationen weitere Grundrechte die Online-Durchsuchung sperren können. Das gilt namentlich für die Pressefreiheit (Art. 5 Abs. 1 Satz 2 GG), die in weitem Umfang auch den Schutz von Informanten umfasst. In Übertragung der Grundsätze des BVerfG zum Fall „Cicero“[55] bedeutet dies, dass nicht nur die herkömmliche Durchsuchung und Beschlagnahme von Unterlagen, sondern auch die Online-Durchsuchung verfassungsrechtlich unzulässig ist, wenn sie ausschließlich oder vorwiegend dem Zweck dient, die Person des Informanten zu ermitteln.[56] Vergleichbare Problemlagen ergeben sich für andere Berufsgeheimnisträger.

4.5 Verhältnismäßigkeit

Wird die Online-Durchsuchung im Ermittlungsverfahren eingesetzt, so richtet sie sich gegen einen konkreten Beschuldigten. Die so erhobenen Daten sind deshalb stets personenbezogen und betreffen sein Grundrecht auf informationelle Selbstbestimmung.[57] Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährt *„die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“*.[58] Einschränkungen sind im überwiegenden Gemeininteresse zulässig, müssen dann aber dem Verhältnismäßigkeitsprinzip genügen.

Die Online-Durchsuchung verfolgt einen legitimen Zweck: Dass BVerfG hat wiederholt die unabweisbaren Bedürfnisse einer wirksamen Strafverfolgung und Verbrechensbekämpfung hervorgehoben.[59] An der Eignung lässt sich angesichts der verfügbaren Schutzinstrumente[60] und des Fehlens von Erfolgsbeispielen[61] zwar zweifeln, sie wird jedoch wegen des Einschätzungsspielraums, den das Gericht dem Gesetzgeber insoweit einräumt, im Ergebnis kaum zu verneinen sein. Allerdings hat dieser bei schweren Grundrechtseingriffen eine Pflicht, die Entwicklung zu beobachten und fortlaufend zu prüfen, ob das Ermittlungsinstrument tatsächlich geeignet ist, auch das mit ihm verfolgte spezielle Ziel in hinreichendem Maße zu erreichen.[62]

Auf der Erforderlichkeitsebene stellt die offene Durchsuchung des Systems – etwa im Rahmen einer Wohnungsdurchsuchung – die mildere Maßnahme dar. Dies hat der 3. Strafsenat entgegen Stimmen in der Literatur[63] überzeugend dargelegt: Die offene Durchsuchung gibt dem Betroffenen die Möglichkeit, die Maßnahme durch Herausgabe einzelner Gegenstände abzuwenden oder in Dauer und Intensität zu begrenzen, ferner ihr bereits während des Vollzugs entgegenzutreten und die Einhaltung ihres angeordneten Umfangs zu überwachen.[64] All dies ist bei heimlichen Maßnahmen nicht möglich.

Daraus folgt, dass die Online-Durchsuchung verfassungsrechtlich nur zulässig ist, wenn die herkömmliche Durchsuchung nebst Beschlagnahme des Computers den Erfolg der Maßnahme vereiteln würde; dies wird in den allermeisten Fällen nicht der Fall sein. Eine Ermächtigungsgrundlage wäre mit einer Subsidiaritätsklausel zu versehen,[65] die neben der herkömmlichen Durchsuchung auch weitere informationstechnische Maßnahmen beinhalten müsste.[66]

Für die objektive Zumutbarkeit sind die Vorteile der Online-Durchsuchung den verursachten Grundrechtsbeeinträchtigungen gegenüberzustellen. Dabei ist nach der Rechtsprechung des BVerfG die Eingriffsintensität maßgeblich zu berücksichtigen; entscheidend ist etwa, wie viele Personen betroffen sind, wie intensiv dies geschieht, ob sie hierfür Anlass gegeben haben, ob sie als Person anonym bleiben, welche Umstände und Inhalte der Kommunikation erfasst werden, welche Nachteile drohen oder nicht ohne Grund befürchtet werden und ob unverdächtige Dritte betroffen sind.[67]

Nach diesen Kriterien ist die Eingriffsintensität als hoch zu beurteilen. Dafür sprechen schon die erwähnte Sensibilität und der Umfang der Daten[68] und die durch die Heimlichkeit der Maßnahme verursachten Rechtsschutzdefizite. Überdies kann – jedenfalls bei der Verwendung von Trojanern, so diese erfolgen sollte – eine Beeinträchtigung Dritter kaum ausgeschlossen werden: Wenn etwa versucht wird, dem Beschuldigten über eine E-Mail einen Trojaner zuzuspielen, so verbleibt immer das Risiko, dass diese über einen Webmail-Dienst vom Rechner eines beliebigen Dritten (Bekannte, Arbeitgeber, Internet-Café) abgerufen wird. Eine zugespielte CD könnte der Beschuldigte an Dritte weitergeben. Beides führt zu erheblichen Problemen, weil es nicht nur die Zielgenauigkeit der Maßnahme beeinträchtigt, sondern auch bei völlig Unbeteiligten Sicherheitslücken in den Systemen verursachen kann und letztlich – wenn der Beschuldigte seine E-Mails im Ausland abruft – sogar Probleme der internationalen Zuständigkeit der deutschen Strafverfolgungsbehörden verursacht.[69] Grundsätzlich abzulehnen ist es in diesem Zusammenhang, den heimlichen Online-Zugriff auf im Ausland befindliche Systeme gerade mit den Beschwerlichkeiten der Rechtshilfeverfahren zu begründen[70] – man stelle sich die Übertragung eines derartigen Grundsatzes auf andere strafprozessuale Maßnahmen vor.

Schließlich hat die Online-Durchsuchung das Potential, die generelle Online-Sicherheit von Bürgern und Wirtschaft[71] und die Kommunikation der Gesellschaft insgesamt[72] zu beeinträchtigen. Mitte März 2007 warnten die in der Exportinitiative „IT

[54] So BVerfG, NJW 2006, 976.

[55] BVerfG, NJW 2007, 1117.

[56] BVerfGE 20, 162 (176, 187 ff.); 36, 193 (204); näher *Rotsch*, Der Schutz der journalistischen Recherche im Strafprozessrecht, 2000; *Rogall*, NJW 1980, 751 ff.; *Behm*, AfP 2000, 421 ff.; *Kugelmann*, ZRP 2005, 260 ff.; *Brüning*, NStZ 2006, 253 ff.; *Birkner/Rösler*, ZRP 2006, 109 ff.

[57] Grundlegend BVerfGE 65, 1. Dieses tritt hier – wie bei der Durchsuchung zur Ermittlung von Kommunikationsdaten (BVerfG, NJW 2006, 976, 979) – nicht hinter Art. 13 GG zurück.

[58] BVerfGE 65, 1 (42).

[59] S. z.B. BVerfGE 77, 65 (76); 100, 313 (389); 107, 299 (316).

[60] S.o. 2 und *Kutscha*, NJW 2007, 1169, 1171; *Gercke*, CR 2007, 245, 248 f.

[61] Schon die Zahl der Anwendungen ist unklar: das BMI spricht von „wenigen Fällen“ (s. *Störing*, c’t 5/2007, 58, 60), die BMJ von vier (SZ vom 15.2.2007); über Erfolg oder Misserfolg gibt es keine öffentlichen Informationen.

[62] BVerfGE 109, 279 (340); ferner BVerfGE 33, 171 (189 f.); 37, 104 (118); 88, 203 (310).

[63] *Graf*, DRiZ 1999, 281, 285; *Hofmann*, NStZ 2005, 121, 124.

[64] BGH, NJW 2007, 930, 931; s.a. *Harrendorf*, StraFo 2007, 149, 150.

[65] S. für die akustische Wohnraumüberwachung BVerfGE 109, 279 (340 ff.).

[66] Vgl. zu weiteren alternativen Ermittlungsinstrumenten *Gercke*, CR 2007, 245, 246 ff.

[67] BVerfGE 109, 279 (353 ff.).

[68] S.o. 4.1.

[69] Die Bundesregierung hat erklärt, durch „intensive Vorbereitung und Vorklärung“ solle „sichergestellt werden, dass der Einsatz im Geltungsbereich des deutschen Rechts erfolgt“ (BT-Drs. 16/4997, 5), jedoch keine Angaben zur Umsetzung gemacht.

[70] So *Bär*, MMR 2007, 239, 242.

[71] S. näher unten 5.

[72] S. zu dieser Dimension allgemein BVerfGE 65, 1 (42 f.); für die akustische Wohnraumüberwachung BVerfGE 109, 279 (354 f.).

Security made in Germany“ zusammengeschlossenen 34 deutschen Anbieter[73] und der Bundesverband Bitkom,[74] bereits das Bekanntwerden der Pläne diskreditiere die deutsche IT-Sicherheitsbranche und unterhöhle ihre Vertrauenswürdigkeit.

Unter diesen Umständen ist die Online-Durchsuchung nur objektiv zumutbar, wenn sie – vergleichbar der akustischen Wohnraumüberwachung – der Verfolgung sehr schwerer Straftaten dient, tatsächliche Anhaltspunkte für die Wahrscheinlichkeit eines Beitrags zum Ermittlungserfolg bestehen und andere Maßnahmen aussichtslos sind. Hinsichtlich der Straftaten lässt sich an die Kriterien des BVerfG zur akustischen Wohnraumüberwachung anknüpfen; danach muss die Tat jedenfalls mit höherer Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt sein.[75]

4.6 Rechtsstaatliche Vorgaben

Neben diesen inhaltlichen Anforderungen bedürfte eine Online-Durchsuchung auch Vorschriften zur verfahrensrechtlichen Absicherung der Grundrechte des Beschuldigten und dritter Personen. Die Durchführung dürfte – anders als im Beispiel von § 5 Abs. 2 Nr. 11 VSG NRW – nur nach richterlicher Anordnung möglich sein.[76] Die Maßnahme wäre zeitlich zu begrenzen. Die erhobenen Daten wären beweissicher zu dokumentieren, zu kennzeichnen und ihre Verwendung wäre auf das laufende Verfahren und die Verfolgung von Straftaten identischen Gewichts zu beschränken.[77] Ein Sicherungsmittel könnte auch die Hinterlegung des Quellcodes der verwendeten Software beim anordnenden Gericht sein.[78]

Ferner wäre die nachträgliche Benachrichtigung der Beschuldigten und betroffener Dritter unabdingbar: Heimliche Eingriffe in das Recht auf Unverletzlichkeit der Wohnung sind mit Art. 13 Abs. 1 und 19 Abs. 4 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nur vereinbar, wenn eine Benachrichtigung grundsätzlich erfolgt und nur in engen Ausnahmefällen unterbleibt.[79] Wenn beispielsweise bei der akustischen Wohnraumüberwachung die Gefährdung der weiteren Verwendung eines verdeckt ermittelnden Beamten die Geheimhaltung nicht rechtfertigen kann,[80] so muss das auch für die Gefährdung der weiteren Verwendung des durch die Behörden für die Online-Durchsuchung verwendeten Computerprogramms gelten.

5 Praktische Risiken

Die Online-Durchsuchung hat noch eine weitere rechtspolitische Dimension. Die Maßnahme erfordert nämlich – unabhängig vom technischen Weg, auf dem die Ermittlungsbehörden sie ausführen – eine Sicherheitslücke in dem adressierten IT-System oder seinen Schutzmechanismen. Das gilt auch bei der Zuspielung von Spionagesoftware über CDs oder andere Trägermedien, da zumindest eine Datenübertragung vom System des Adressaten erforderlich ist. Da jedoch kaum zu erwarten ist, dass diese Lücke nur den Behörden bekannt ist, stehen diese vor einem Dilemma: Während es im Rahmen der Kriminalitätsvorsorge zu ihren Aufgaben gehört, Privatpersonen und Wirtschaft entsprechend zu warnen und so Angriffen zu Zwecken der Wirtschaftsspionage, aus Geltungssucht einzelner Hacker oder zu anderen Motiven vorzubeugen, besteht nunmehr die Gefahr eines Interesses daran, Sicherheitslücken nicht publik werden zu lassen, Schutzmechanismen nicht mit letzter Genauigkeit zu implementieren oder entsprechendes Wissen nicht allgemein bekannt werden zu lassen.[81]

Dieser Widerspruch zeigt sich besonders bei der Rolle des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), das nach § 3 BSIG zugleich Polizei, Strafverfolgungs- und Verfassungsschutzbehörden bei ihrer Arbeit unterstützen (Nr. 6) und Hersteller, Vertreiber und Anwender in Fragen der Sicherheit der Informationstechnik beraten soll (Nr. 7).[82] Wäre die Online-Durchsuchung zulässig, bestünde die Gefahr eines doppelten Vertrauensverlusts: Zum einen wäre unklar, ob man den regelmäßigen Sicherheitswarnungen des BSI – jedenfalls hinsichtlich ihrer Vollständigkeit – trauen könnte, zum anderen könnte letztlich das grundsätzliche Vertrauen in die Sicherheit von IT-Infrastrukturen unterminieren werden.

Seitens der Bundesregierung hat man das Problem offensichtlich erkannt und plant, die Maßnahmen ohne Unterstützung des BSI durchzuführen.[83] Das grundsätzliche Dilemma der Rolle der beteiligten Behörden wird dadurch jedoch nicht gelöst, wie sich an den oben erwähnten Bedenken deutscher Anbieter der IT-Sicherheitsbranche und Warnungen seitens der Unternehmen vor der Gefahr einer Förderung der Wirtschaftsspionage zeigt.[84] Immerhin brachte die Entscheidung des 3. Strafsenats des BGH den Anbieter von IT-Sicherheitsprodukten Sophos dazu, auf seiner Internetseite zu erklären, „seine Produkte auch für staatliche Trojaner nicht löchrig machen zu wollen“.[85]

6 Ausblick

De lege lata sperrt Art. 13 GG eine einfachgesetzliche Ermächtigungsgrundlage für die Online-Durchsuchung. Dies gilt vollständig, da den Ermittlungsbehörden der Standort des IT-Systems regelmäßig nicht bekannt sein wird, sie jedoch damit rechnen müssen, dass dieser innerhalb des von Art. 13 GG geschützten Bereichs liegt und weder sie noch der Gesetzgeber einen rechtswidrigen Eingriff in das Grundrecht billigend in Kauf nehmen dürfen.

Die größte Hürde an eine Verfassungsänderung und nachfolgende Ermächtigung liegt im Schutz des Kernbereichs privater Lebensgestaltung. Für dessen Gewähr sind bislang kaum praktikable Mechanismen erkennbar. Vor dem Hintergrund dieser Schwierigkeiten, der engen weiteren Vorgaben für eine Ermächtigungsgrundlage und dem beschriebenen Risiko des Vertrauensverlusts in die IT-Sicherheit sollte der Gesetzgeber von dem Vorhaben zumindest solange absehen, wie die tatsächliche ermittlungstechnische Eignung und Notwendigkeit der Online-Durchsuchung nicht in sehr viel deutlicherer Art plausibel gemacht worden sind als bisher.

[73] http://www.itsmig.de/news/news.php?nid=398.

[74] http://www.heise.de/newsticker/meldung/88659.

[75] BVerfGE 109, 279 (347 f.).

[76] Zur Funktion des Richtervorbehalts BVerfGE 109, 279 (357 ff.); ferner BVerfGE 103, 142 (151); 107, 299 (325).

[77] Zu den verfassungsrechtlichen Grenzen solcher Zweckänderungen BVerfGE 109, 279 (374 ff.).

[78] Dies wird von BKA-Präsident *Ziercke* angeregt, s. http://www.heise.de/newsticker/meldung/87421.

[79] BVerfGE 109, 279 (363 ff.).

[80] BVerfGE 109, 279 (366).

[81] *Schaar/Landwehr*, K&R 2007, 202, 205.

[82] Zu diesem „Geburtsfehler“ des BSI *Bizer/Hammer/Pordesch/Roßnagel*, DuD 1990, 178 ff.

[83] BT-Drs. 16/4997, 3.

[84] S. Computerzeitung vom 12.2.2007.

[85] Vgl. http://de.internet.com/index.php?id=2047643 &section=Security.