Deutscher Bundestag ■ Wissenschaftliche Dienste

Verfassungsmäßigkeit von Online-Durchsuchungen

- Ausarbeitung -

[redacted]

Wissenschaftliche Dienste des Deutschen Bundestages

Verfasser/in: [redacted]

Verfassungsmäßigkeit von Online-Durchsuchungen

Ausarbeitung WD 3 - 161/07

Abschluss der Arbeit: 7.5.2007

Fachbereich WD 3: Verfassung und Verwaltung

Telefon: [redacted]

- Zusammenfassung -

Die so genannte **Online-Durchsuchung** ist **keine klar definierte Ermittlungsmaßnahme**. Technisch sind **unterschiedliche Überwachungswege** und **Überwachungsarten** möglich.

Jede zurzeit diskutierte **Online-Durchsuchung greift** in **Grundrechte** ein. Das **Recht auf informationelle Selbstbestimmung** ist unstreitig betroffen, das **Fernmeldegeheimnis** nur in bestimmten Konstellationen.

Ob darüber hinaus auch das **Recht der Unverletzlichkeit der Wohnung** betroffen ist, wird unterschiedlich beurteilt. Da hierzu einschlägige Rechtsprechung der Verfassungsgerichte bislang fehlt, ist eine abschließende Bewertung nicht möglich. Die **Intensität der Beeinträchtigung** durch heimliche Online-Durchsuchungen ist jedoch mit Eingriffen in Art. 13 Abs. 1 GG **vergleichbar**.

Rechtsgrundlagen für eine Online-Überwachung existieren derzeit **nur in Nordrhein-Westfalen** im Verfassungsschutzgesetz; **im Übrigen** gibt es **keine Eingriffsgrundlage**. Dies gilt für Gefahrenabwehr in Bund und Ländern sowie nach überwiegender Auffassung für Strafverfolgungsmaßnahmen.

Bei der Schaffung einer Eingriffsgrundlage sind **strenge Maßstäbe** an **Bestimmtheit**, **Verhältnismäßigkeit** und **Maßnahmen zum Schutz** des **absolut geschützten Kernbereichs privater Lebensgestaltung** anzulegen. Es bedarf – ähnlich wie bei der akustischen Wohnraumüberwachung – einer **qualifizierten Rechtsgrundlage**.

Inhalt

W

1. Tatsächliche Grundlagen und Begriffsklärungen

Bei der so genannten Online-Durchsuchung handelt es sich nicht um eine klar definierte Ermittlungsmaßnahme.[1] Vielmehr sind **aus technischer Sicht verschiedene Arten des heimlichen Fernzugriffs** auf Computersysteme denkbar.[2] Möglich wäre beispielsweise, bekannte Sicherheitslücken eines Systems durch einen „**Virus**“ – ein unerwünschtes Schadprogramm – zu **infiltrieren**.[3] In Betracht kommt auch, in jedes Betriebssystem eine Schnittstelle zu integrieren, durch die staatliche Stellen Zugriff auf das System nehmen könnten.[4]

Außerdem können **verschiedene Ermittlungsarten** unterschieden werden:

Zunächst kommt ein **einmaliger Zugriff auf die gespeicherten Daten** in Betracht, etwa die Suche nach einzelnen Dateien oder eine Komplettkopie eines Datenträgers. Ähnlich wie bei der Beschlagnahme erhalten die Ermittler eine Momentaufnahme des Datenträgers.[5]

Denkbar ist weiterhin, dass die Ermittler den **Datenbestand kontinuierlich beobachten**, **Änderungen verfolgen** und auf **Dateien** zugreifen, die nur für eine **begrenzte Zeit** gespeichert werden.[6] Außerdem könnte so auf **verschlüsselte Dateien** zugegriffen werden, wenn der Nutzer den Zugang frei schalten wird.[7]

Schließlich könnten **neben der reinen Datenspeicherung und Datenüberwachung** beispielsweise noch folgende Maßnahmen vorgenommen werden[8]:

- durch einen Sniffer oder Keylogger[9] könnten **Passwörter** ausgelesen werden,
- **Internet-Telefonie** könnte am Rechner mitgeschnitten werden,
- **Mikrofone und Kameras der Computer** könnten aktiviert und zur Überwachung der Wohnung genutzt werden,
- der **Rechner** könnte **ferngesteuert** und so beispielsweise der Abruf von E-Mails initiiert werden.

---

1 Buermeyer, HRR-Strafrecht 2007, 154, beigefügt als Anlage 1; Jahn/Kudlich, JR 2007, 57 (58).

2 Eine sehr gut verständliche Darstellung der technischen Möglichkeiten bietet Buermeyer, HRR-Strafrecht 2007, 154 (155 ff., 163 ff.), beigefügt als Anlage 1.

3 „Bundes-Trojaner“, vgl. Buermeyer, HRR-Strafrecht 2007, 154 (163).

4 „Bundes-Backdoor“, vgl. Buermeyer, HRR-Strafrecht 2007, 154 (163).

5 Buermeyer, HRR-Strafrecht 2007, 154 (160), beigefügt als Anlage 1.

6 Buermeyer, HRR-Strafrecht 2007, 154 (161), beigefügt als Anlage 1.

7 Buermeyer, HRR-Strafrecht 2007, 154 (161), beigefügt als Anlage 1.

8 Beispiele mit Erläuterungen bei Buermeyer, HRR-Strafrecht 2007, 154 (161 f.), beigefügt als Anlage 1; zur *„Vielgestaltigkeit technischer Zugriffsmöglichkeiten“*, Jahn/Kudlich, JR 2007, 57 (58).

9 Begriffe erläutert bei Buermeyer, HRR-Strafrecht 2007, 154 (157), beigefügt als Anlage 1.

Die Ermittlungsmaßnahmen bei einer Online-Untersuchung sind dementsprechend nicht homogen und entfalten **unterschiedliche Eingriffsintensität**. Das ist für die verfassungsrechtliche Beurteilung zu beachten, da die **unterschiedlichen Maßnahmen verschiedene Grundrechte** betreffen können (siehe unten 2.).

Der **Begriff** „Online-Durchsuchung" ist **missverständlich**, weil es sich wohl nicht um einen Fall der Durchsuchung nach §§ 102 ff. StPO handelt.[10] Treffender wäre der Begriff „Online-Überwachung". Im Folgenden wird aber der nunmehr gebräuchlichere Begriff „Online-Durchsuchung" verwandt.

2. Grundrechtsrelevanz

2.1. Vorbemerkung

Dass eine heimliche Online-Durchsuchung in Grundrechte **eingreift**, ist unbestritten[11]; **strittig** ist, **welche Grundrechte** betroffen sind. Die Frage ist nicht nur dogmatischer Natur, da aus dem einschlägigen Grundrecht die zu beachtende Schranke folgt[12]. Die hier untersuchten Grundrechte sind hinsichtlich des **Schutzes der persönlichen Lebenssphäre** am speziellsten.[13]

2.2. Art. 10 Abs. 1 GG, Fernmeldegeheimnis

Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG gewährleistet die **Vertraulichkeit der individuellen Kommunikation**, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter ermöglicht.[14] Das **Fernmeldegeheimnis** ist wesentlicher Bestandteil des Schutzes der Privatsphäre und **gewährleistet eine Privatheit auf Distanz**.[15] Es schützt die **unkörperliche Übermittlung von Informationen** an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs; die Beteiligten sollen weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwe-

---

10 So ausdrücklich Brigitte Zypries, Bundesjustizministerin, in einer Rede beim Europäischen Polizeikongress am 13.2.2007, www.bmj.bund.de; siehe auch Kutscha, NJW 2007, 1169 (1169).

11 Statt vieler: Rux, JZ 2007, 285 (287), beigefügt als Anlage 2; Brigitte Zypries, Bundesministerin der Justiz, in einer Rede beim Europäischen Polizeikongress am 13.2.2007, www.bmj.bund.de.

12 Vgl. nur die Schrankensystematik des Art. 13 GG mit der Unterscheidung nach der Art der Maßnahme (Art. 13 Abs. 2 GG, Durchsuchung) oder der Zielrichtung des Eingriffs (Art. 13 Abs. 3 und 4 GG, repressive und präventive Maßnahmen).

13 Daneben wird überlegt, ob in bestimmten Fällen auch der Justizgewähranspruch aus Art. 19 Abs. 4 GG, die Pressefreiheit aus Art. 5 Abs. 1 S. 2 GG oder die Berufsfreiheit aus Art. 12 Abs. 1 GG tangiert sein könnte, vgl. Baum/Reiter/Schantz, S. 30 ff.; Roggan, S. 24 ff.

14 BVerfG, NJW 2006, 976 (978), beigefügt als Anlage 3; Löwer, in: v. Münch/Kunig, GG, Art. 10, Rn. 11, 18; Gusy, in: v. Mangoldt/Klein/Starck, GG, Art. 10, Rn. 45.

15 Gusy, in: v. Mangoldt/Klein/Starck, GG, Art. 10, Rn. 19.

senden stünden.[16] Das **Grundrecht ist entwicklungsoffen** und umfasst **auch neuartige Übertragungstechniken**.[17]

Bei der Online-Durchsuchung ist zu unterscheiden: Geht es um einen reinen **Datenabgleich** oder eine dauerhafte Überwachung bereits gespeicherter Dateien, wird nach wohl überwiegender Auffassung **nicht die Kommunikation** zwischen einem Verdächtigen und einem Dritten **überwacht**.[18] Vielmehr wird zielgerichtet eine umfassende Übermittlung solcher Daten ausgelöst, die vor dem Beginn des Telekommunikationsvorgangs auf dem Zielcomputer gespeichert waren.[19] Der **Datenfluss** während des Online-Status des Computers wird somit **lediglich aus technischen Gründen** zum Zwecke der Übertragung der abgelegten Dateien benutzt.[20]

Wenn ein Gespräch über **Internet-Telefonie**[21] **mitgehört**, eine **Email automatisch weitergeleitet** oder der **Abruf** von einem externen Email-Server **beobachtet** oder initiiert werden würde[22], kommt indes ein Eingriff in Art. 10 Abs. 1 GG in Betracht. Diese Fälle sind vergleichbar mit dem Abhören am Endgerät; bei bestimmten Maßnahmen hat das Bundesverfassungsgericht einen Eingriff in das Fernmeldegeheimnis bejaht.[23]

2.3. Art. 13 Abs. 1 GG, Unverletzlichkeit der Wohnung

Art. 13 GG schützt die **Unverletzlichkeit der Wohnung**. Dieses Grundrecht verbürgt dem Einzelnen einen **elementaren Lebensraum** und gewährleistet das **Recht**, in diesem Raum **in Ruhe gelassen zu werden**.[24] Art. 13 Abs. 1 GG schützt somit die **räumliche Privatsphäre** insbesondere in Gestalt eines Abwehrrechts.[25] Die Norm enthält das an Träger öffentlicher Gewalt gerichtete grundsätzliche **Verbot**, gegen den Willen des Wohnungsinhabers **in die Wohnung einzudringen** und darin zu verweilen.[26] Außer-

16 BVerfG, NJW 2006, 976 (978), beigefügt als Anlage 3.

17 Vgl. BVerfGE 46, 120 (144). Dabei kommt es nicht auf die konkrete Übermittlungsart (Kabel oder Funk, analoge oder digitale Übermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) an, BVerfG, NJW 2006, 976 (978), beigefügt als Anlage 3.

18 Rux, JZ 2007, 285 (292), beigefügt als Anlage 2; Huster, S. 3; differenzierend Bär, MMR 2007, 175 (176): kritisch: Störing, CR 2007, 392 (393).

19 Für Verbindungsdaten siehe BVerfG, NJW 2006, 976 (978), beigefügt als Anlage 3; anders noch der Kammerbeschluss vom 4.2.2005 zur Beschlagnahme eines Mobiltelefons zur Auslesung der SIM-Karte, BVerfG, NStZ 2005, 337 (338 f.).

20 BGH, Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, Rn. 18, beigefügt als Anlage 4a.

21 „Voice-over-IP“, ausführliche Hinweise zu technischen Fragen und Sicherheitsaspekten unter http://www.verbraucherzentrale-rlp.de/UNIQ117819974231623/link198209A.html, letzter Abruf am 3.5.2007.

22 Vgl. Baum/Reiter/Schantz, S. 25; zustimmend mit weiteren Beispielen Rux, JZ 2007, 285 (287), beigefügt als Anlage 2.

23 BVerfG, NJW 2006, 976 (979), beigefügt als Anlage 3.

24 BVerfGE 32, 54 (75); BVerfGE 42, 212 (219); 51, 97 (110).

25 Vgl. BVerfGE 7, 230 (238); BVerfGE 65, 1 (40).

26 Vgl. BVerfGE 76, 83 (89 f.)

dem beinhaltet sie das **Verbot**, **Abhörgeräte** in der **Wohnung** zu **installieren** oder sie zu **benutzen**[27]:

> *„Im Zeitpunkt der Schaffung des Grundgesetzes diente das Grundrecht des Art. 13 I GG primär dem Schutz des Wohnungsinhabers vor unerwünschter physischer Anwesenheit eines Vertreters der Staatsgewalt. Seitdem sind neue Möglichkeiten für Gefährdungen des Grundrechts hinzu gekommen. 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 Absatz 1 umfasst wäre.“*[28]

Für die Online-Durchsuchung wird die Betroffenheit von Art. 13 Abs. 1 GG[29] unterschiedlich beurteilt. **Einigkeit** dürfte nur insoweit bestehen, als Art. 13 Abs. 1 GG einschlägig ist, wenn der **Rechner als Abhörsystem** dazu genutzt wird, um Vorgänge oder Zustände innerhalb der Wohnung, aber außerhalb des Rechners zu erforschen.[30] Außerdem geht die überwiegende Auffassung davon aus, dass allein der **Zugang zum Internet keinen Grundrechtsverzicht** darstellt.[31] Die Richtigkeit dieser Auffassung ergibt sich schon daraus, dass ein Zugriff auf einen Rechner eines Dritten regelmäßig unter Umgehung von Sicherheitsvorkehrungen geschieht.[32] Im Übrigen verzichtet auch derjenige nicht auf den Schutz des Art. 13 Abs. 1 GG, der Haus- oder Wohnungstüren unverschlossen lässt.

Zu der Frage, ob bei einer Online-Durchsuchung des Computers der **Schutzbereich** von **Art. 13 Abs. 1 GG betroffen** ist, gibt es **bislang keine ausdrückliche Rechtsprechung** des Bundesverfassungsgerichts.[33] In der **Literatur** werden im Wesentlichen **drei Positionen** vertreten.

---

27 Vgl. BVerfGE 65, 1 (40).

28 BVerfG, NJW 2004, 999 (1001).

29 Insbesondere mit Bezug auf das oben stehende Zitat.

30 Gusy, S. 6; zur technischen Möglichkeit vgl. Buermeyer, HRR-Strafrecht 2007, 154 (161 f.), beigefügt als Anlage 1.

31 So aber Hofmann, NStZ 2005, 121 (124).

32 Firewall und Antivirenprogramm, vgl. Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/fachthem/sinet/loesungen_netze/index.htm, letzter Aufruf am 3.5.2007; Kutscha, NJW 2007, 1169 (1170); Baum/Reiter/Schantz, S. 27; siehe auch § 202a StGB und die Begründung des Gesetzentwurfs (Strafrechtsänderungsgesetz) der Bundesregierung zur Bekämpfung der Computerkriminalität vom 30.11.2006, BT-Drs. 16/3656, S. 9.

33 Der BGH, Beschluss vom 21.2.2006, Aktenzeichen 3 BGs 31/06, beigefügt als Anlage 4c, hat einen Eingriff in den Schutzbereich verneint; im Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, beigefügt als Anlage 4a, wurde die Frage offen gelassen; das BMJ prüft die Rechtslage, vgl. Zypries,

W

2.3.1. Keine Betroffenheit von Art. 13 Abs. 1 GG

Nach einer Auffassung stellt das Eindringen in fremde Rechnersysteme **regelmäßig keinen Eingriff** in Art. 13 Abs. 1 GG dar. Das gelte jedenfalls, solange es sich alleine um ein Eindringen in technische Kommunikationsbeziehungen handele.[34] Solche Kommunikationsbeziehungen seien nicht von Art. 13 Abs. 1 GG geschützt; vielmehr schütze Art. 13 Abs. 1 GG gegen **Beeinträchtigungen der räumlichen Sphäre**.[35]

Der Schutz eines Computers hänge ansonsten von seinem Standort ab; dieser sei aber aufgrund von tragbaren Computern und W-Lan-Netzen[36] zunehmend zufällig[37]. Schließlich beeinflusse der Zugriff über das Internet nicht die Stätte des räumlichen Lebens und Wirkens.[38]

2.3.2. Partielle Betroffenheit von Art. 13 Abs. 1 GG

Eine weitere Auffassung geht von einem **Eingriff in Art. 13 Abs. 1 GG** aus, wenn sich der **Rechner in einem durch Art. 13 Abs. 1 GG geschützten Raum** befindet.[39] Der Wohnungsinhaber vertraue darauf, dass die Gegenstände, die sich innerhalb seiner Wohnung befinden, einen besonders hohen Schutz genießen. Das gelte auch für **Dateien auf dem Rechner**, da viele vertrauliche Informationen, die früher in körperlicher Form in der Wohnung aufbewahrt wurden und damit unstreitig in den räumlichen Schutzbereich der Wohnung fielen, heute auf dem heimischen Computer gespeichert werden.[40]

Im Ergebnis könne zwischen einem **Brief, der sich ausgedruckt und abgeheftet** in der Wohnung befindet und einem **Brief, der sich auf der Festplatte des Rechners befindet**, **kein Unterschied** bestehen.[41] Die technische Entwicklung dürfe nicht zu einer Absenkung des Niveaus des Grundrechtsschutzes führen.

Brigitte, Bundesministerin der Justiz, in einer Rede beim Europäischen Polizeikongress am 13.2.2007, www.bmj.bund.de.

34 Gusy, S. 6; Roth, S. 18; Schwarz, S. 5.

35 Gusy, S. 6; Lorentz, S. 6 ff.; Böckenförde, S. 224; Hofmann, NStZ 2005, 121 (125). Soweit auf BVerfG, NJW 2006, 976 ff. (beigefügt als Anlage 3) rekurriert wird, ist zu beachten, dass hier maßgeblich die Abgrenzung zwischen Art. 10 Abs. 1 GG und Art. 2 Abs. 1, Art. 1 Abs. 1 GG für die auf dem Rechner bereits gespeicherten Verbindungsdaten war. Das BVerfG ist aber davon ausgegangen, dass die Durchsuchung auch an Art. 13 Abs. 1 und 2 GG zu messen war, vgl. BVerfG, NJW 2006, 976 (981 f.), beigefügt als Anlage 3.

36 Wireless LAN = drahtloses lokales Netz, vgl. Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/fachthem/sinet/basis/basis_WLAN.htm, letzter Aufruf am 3.5.2007.

37 Germann, S. 541; Böckenförde, S. 224; Beulke, StV 2007, 63 (64).

38 Böckenförde, S. 224.

39 Kutscha, NJW 2007, 1169 (1170); Jahn/Kudlich, JR 2007, 57 (60); Baum/Reiter/Schantz, S. 25; Huster, S. 4; Roggan, S. 19; Bär, MMR 2007, 175 (176).

40 Zahlreiche Beispiele bei Hornung, CR 2007, 144 (144); Baum/Reiter/Schantz, S. 26; Roggan, S. 20; siehe auch BVerfG, NJW 2006, 976 (980), beigefügt als Anlage 3.

41 Sokol, S. 10.

W

2.3.3. Mit Eingriffen in Art. 13 Abs. 1 GG vergleichbare Betroffenheit

Schließlich wird vertreten, dass die Ausforschung privater Rechner in **Intensität und Intension vergleichbar** sei mit einem Eingriff in das Recht auf Unverletzlichkeit der Wohnung.[42] Dementsprechend müssten die **Schranken von Art. 13 GG entsprechend** zur Anwendung kommen[43] **oder** aber, wenn man diese nicht für einschlägig hält, eine **Änderung der Verfassung** vorgenommen werden[44].

2.4. Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Informationelle Selbstbestimmung

Durch den heimlichen Zugriff auf Computerdaten wird – unabhängig von der konkreten Art des Zugriffs – in das **Recht auf informationelle Selbstbestimmung** eingegriffen.[45]

Dieses Recht hat das Bundesverfassungsgericht aus dem **Allgemeinen Persönlichkeitsrecht** des **Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG** hergeleitet und ausgeführt:

> *„Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient (...) das in Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG gewährleistete allgemeine Persönlichkeitsrecht, das gerade auch im Blick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen der menschlichen Persönlichkeit Bedeutung gewinnen kann (...) Es umfaßt (...) auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen,* ***grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden*** *(...).“*[46]

3. Ermächtigungsgrundlagen im derzeit geltenden Recht

Hinsichtlich möglicher Rechtsgrundlagen ist zwischen verschiedenen Arten staatlichen Handelns zu unterscheiden: Maßnahmen zur **Gefahrenabwehr** auf Bundes- und auf Länderebene sowie Maßnahmen zur **Strafverfolgung**.

---

42 Rux, JZ 2007, 285 (292 ff.), beigefügt als Anlage 2; Kaufmann, MMR 2007, 175; so auch Wiefelspütz, Dieter, *„Online-Überwachung, Ja aber ...“*, Interview mit Cicero, vgl. http://www.cicero.de/259.php?kol_id=10283, letzter Abruf am 4.5.2007.

43 So genannte Schrankentransplantation. Denkbar wäre auch eine erweiternde Auslegung des Begriffes „Wohnung“ im Sinne einer virtuellen Umgebung, die ebenfalls von Art. 13 Abs. 1 GG erfasst wäre, zu beiden Ansätzen Rux, JZ 2007, 285 (293, 295), beigefügt als Anlage 2.

44 So Jahn/Kudlich, JR 2007, 57 (60); sowie Marxen, Klaus (Hrsg.), *„Fall des Monats“* der Humboldt-Universität zu Berlin, Ausgabe März 2007, S. 5, abrufbar unter www.fall-des-monats.de.

45 BGH, Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, beigefügt als Anlage 4a; Beulke, StV 2007, 63 (64); zum offenen Zugriff auf Computerdaten bei einer Durchsuchung, der Abgrenzung zu Art. 10 Abs. 1 GG und dem Verhältnis zu Art. 13 Abs. 1 GG vgl. BVerfG, NJW 2006, 976 ff., beigefügt als Anlage 3 sowie BVerfG, NJW 2005, 1917 ff. zur Beschlagnahme von Datenträgern bei Berufsgeheimnisträgern.

46 BVerfGE 65, 1 (41 f.), (Hervorhebung durch die Verfasserin).

W

3.1. Gefahrenabwehrrecht und geheimdienstliche Maßnahmen

3.1.1. Polizeiliche und geheimdienstliche Maßnahmen nach Bundesrecht

Zur Verhütung von Straftaten und damit zu **präventiven Zwecken** gibt es nach geltendem Recht für die **Polizeibehörden des Bundes keine Rechtsgrundlage** für eine Online-Durchsuchung.[47]

Nach Auffassung der Bundesregierung[48] sind Rechtsgrundlagen für eine Online-Durchsuchung durch das **Bundesamt für Verfassungsschutz** die §§ 9 Abs. 1, 8 Abs. 2 Bundesverfassungsschutzgesetz[49] (BVerfSchG).

Die Befugnis des **Militärischen Abschirmdienstes** soll aus den §§ 5, 4 Abs. 1 des Gesetzes über den Militärischen Abschirmdienst[50] (MADG) i.V.m. §§ 9 Abs. 1, 8 Abs. 2 BVerfSchG folgen[51].

Für den **Bundesnachrichtendienst** enthalte § 3 des Gesetzes über den Bundesnachrichtendienst[52] (BNDG), der auf § 8 Abs. 2 BVerfSchG Bezug nimmt, eine ausreichende Rechtsgrundlage[53].

In Ergänzung zu den genannten Normen soll seit 2005 eine **Dienstvorschrift des Bundesinnenministers** dem Bundesamt für Verfassungsschutz erlaubt haben, heimlich auf

---

47 Antwort der Bundesregierung auf eine Kleine Anfrage, BT-Drs. 16/3972, S. 2; Tätigkeitsbericht des Bundesbeauftragten für Datenschutz und Informationsfreiheit, BT-Drs. 16/4950, S. 64 f.

48 BT-Drs. 16/4803, S. 8; zustimmend (allerdings ohne weitere Nachweise) Germann, S. 547 ff.; zurzeit prüft die Bundesregierung, welche Rechtsgrundlagen bestehen, vgl. BT-Drs. 16/4997, S. 2.

49 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20.12.1990, BGBl. I 2954, zuletzt geändert durch Art. 1, Art. 10 Abs. 1 des Terrorismusbekämpfungsergänzungsgesetzes vom 5.1.2007, BGBl. I 2, vgl. Anlage 5.

50 Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz – MADG), vom 20.12.1990, BGBl. I 2954, zuletzt geändert durch das Terrorismusbekämpfungsergänzungsgesetz vom 5.1.2007, BGBl. I 2, 4, vgl. Anlage 5.

51 BT-Drs. 16/4803, S. 8.

52 BT-Drs. 16/4803, S. 9.

53 Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG), vom 20.12.1990, BGBl. I 2954, zuletzt geändert durch das Terrorismusbekämpfungsergänzungsgesetz vom 5.1.2007, BGBl. I 2, 4, 8, vgl. Anlage 5.

Computersysteme zuzugreifen.[54] Diese **Dienstanweisung liegt** den Wissenschaftlichen Diensten **nicht** vor.[55]

Unabhängig vom Inhalt einer Dienstanweisung gilt jedoch der **Vorbehalt des Gesetzes**[56]: Staatliche Maßnahmen, die in Grundrechte eingreifen, bedürfen grundsätzlich einer **gesetzlichen** Ermächtigung.[57]

Speziell für Online-Durchsuchungen ist davon auszugehen, dass diese Grundrechtseingriffe einer **speziellen Ermächtigung** bedürfen.[58]

Dafür plädiert auch die überwiegende Auffassung in der Literatur: **Generalklauselartige Ermächtigungen** zur Datenerhebung **reichten** als Grundlage für die Online-Durchsuchung **nicht aus**. Dies gelte umso mehr, als der Gesetzgeber in den vergangenen Jahren durchweg dazu übergangen sei, **besondere Formen der Datenerhebung** auch **ausdrücklich zu regeln**.[59] Außerdem sprächen die **zahlreichen Möglichkeiten** der technischen Überwachung[60] (siehe oben 1.) und die damit verbundene **Eingriffstiefe**[61] für die Notwendigkeit ausdrücklicher und hinreichend bestimmter Eingriffsgrundlagen[62].

---

54 Siehe hierzu die ausführliche Meldung aus dem Innenausschuss in „heute im bundestag“ vom 25.4.2007, http://www.bundestag.de/aktuell/hib/2007/2007_108/03.html, letzter Abruf am 4.5.2007; der ehemalige Staatssekretär des Bundesinnenministers Otto Schily, Lutz Diwell (BMJ) geht indes davon aus, dass die Dienstanweisung gar keine heimliche Überwachung privater Rechner erlauben sollte, vgl. Rath, Christian, „Online-Schnüffeln ohne Freibrief?“, in: die Tageszeitung vom 2.5.2007; siehe auch Interview mit Brigitte Zypries, Bundesjustizministerin, in: Die Welt vom 7.5.2007.

55 Laut telefonischer Auskunft des Parlaments- und Kabinettsreferats des Bundesministeriums des Innern vom 4.5.2007 ist die Dienstanweisung als *„Vertraulich, nur für den Dienstgebrauch“* eingestuft und wurde deshalb nicht zur Verfügung gestellt.

56 Sommermann, in: v. Mangoldt/Klein/Starck, GG, Art. 20 Abs. 3, Rn. 273 ff., m.w.N.

57 Sommermann, in: v. Mangoldt/Klein/Starck, GG, Art. 20 Abs. 3, Rn. 276, m.w.N.

58 Rux, JZ 2007, 285 (288), beigefügt als Anlage 2; allgemein bezüglich neuerer Kommunikationsmethoden, Löwer, in: v. Münch/Kunig, GG, Art. 10, Rn. 40 a.E.

59 Rux, JZ 2007, 285 (288), beigefügt als Anlage 2. Vgl. z.B. für die (weniger eingriffsintensive) Videoüberwachung öffentlicher Orte § 24a ASOG Berlin sowie Überblick bei Zöller, NVwZ 2005, 1235 (1236); Wohlfarth, LKRZ, 54 (55 ff.).

60 Siehe dagegen die allgemeine Formulierung des § 8 Abs. 2 S. 1 BVerfSchG, der heimliche Informationsbeschaffung wie z.B. den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen erlaubt.

61 *„(…) teile ich Ihre Auffassung, dass es sich (…) um einen sehr tief greifenden Eingriff handelt.“*, Hartenbach, Alfred, Parlamentarischer Staatssekretär bei der Bundesministerin der Justiz, Plenarprotokoll 16/72, S. 7170 (C); a.A. Graf, DRiZ 1999, 281 (285).

62 Jahn/Kudlich, JR 2007, 57 (58); Hornung, CR 2007, 144 (144); Bär, MMR 2007, 175 (177); allgemein zu den Anforderungen an den Bestimmtheitsgrundsatz auch Gusy, Auswirkungen des Lauschangriffsurteils, 35 (39).

Soweit vertreten wird, dass die Nachrichtendienste sich auf eine Generalklausel stützen könnten[63], steht dieser Position Verfassungsgerichtsrechtsprechung entgegen:

> *„**Für schwerwiegende Grundrechtseingriffe** (...) **müssen** daher **die Voraussetzungen und Schranken**, unter denen der Eingriff vorgenommen werden darf, **im Gesetz für den Rechtsanwender erkennbar geregelt sein**.“*[64]

3.1.2. Polizeiliche und geheimdienstliche Maßnahmen nach Landesrecht

Das Land Nordrhein-Westfalen hat als **einziges Bundesland** die Online-Durchsuchung ausdrücklich geregelt.[65] Im **Verfassungsschutzgesetz**[66] findet sich in § 5 Abs. 2 Nr. 11 die **Möglichkeit der verdeckten Datenerhebung**, die ausweislich der Begründung zu diesem Gesetz[67] den Zugriff auf gespeicherte Computerdaten ermöglichen soll. Insbesondere aufgrund dieser Vorschrift sind bereits zwei **Verfassungsbeschwerden** eingelegt worden.[68]

3.2. Strafverfolgung

Der **Bundesgerichtshof** hat in drei Entscheidungen Aussagen zur Online-Durchsuchung getroffen.[69] Er ist zuletzt zum Ergebnis gekommen, dass es **derzeit kei-**

---

63 Germann, S. 548: *„Somit ist der Weg grundsätzlich frei, auch das heimlich Auslesen von Daten über das Computernetz als ‚Methode zur heimlichen Informationsbeschaffung' zu den von der nachrichtendienstlichen Generalklausel gedeckten Maßnahmen zu rechnen.“*

64 SächsVerfGH, NVwZ 2005, 1310 (1313), zum „Großen Lauschangriff“ durch den Verfassungsschutz des Landes, (Hervorhebung durch die Verfasserin); allgemein zur Reichweite des § 8 Abs. 2 BVerfSchG, Sachs, GG, Art. 87, Rn. 44.

65 Im Übrigen gibt es nach derzeitigem Erkenntnisstand im Polizei- und Ordnungsrecht keine taugliche Ermächtigung, vgl. Leipold, NJW-Spezial 2007, 135 (136); Germann, S. 545 f.; ausführliche Prüfung für Baden-Württemberg bei Rux, JZ 2007, 285 (289), beigefügt als Anlage 2; siehe auch Aktuelle Stunde zum Thema Online-Durchsuchung im Landtag Rheinland-Pfalz, Plenarprotokoll 15/18, S. 980 ff; Antwort der Landesregierung Mecklenburg-Vorpommern auf eine Kleine Anfrage, LT-Drs. 5/298; zur Zahl der Online-Durchsuchungen in Bayern vgl. LT-Drs. 15/7502, S. 4; Kleine Anfrage im Landtag Nordrhein-Westfalen zu Online-Durchsuchungen vor der Änderung des Verfassungsschutzgesetzes, LT-Drs. 14/4254; Initiative Thüringens im Bundesrat für die Schaffung einer Rechtsgrundlage, vgl. Pressemitteilung 19/2007, www.thüringen.de.

66 Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (Verfassungsschutzgesetz Nordrhein-Westfalen – VSG NRW), vom 20.12.1994, GV. NW. 1995, S. 28, zuletzt geändert durch ÄndG vom 20.12.2006, GV. NRW. S. 620, vgl. Anlage 5.

67 Landtags-Drucksache 14/2211, S. 17; eine Zusammenfassung der Stellungnahmen der Sachverständigen findet sich in der Landtagsdrucksache 14/3045, S. 5 ff.

68 Antragsschrift der Verfassungsbeschwerden Baum/Reiter/Schantz und Roggan abrufbar unter: http://www.hrr-strafrecht.de/hrr/doku/2007/001/index.php, letzter Aufruf am 2.5.2007.

69 BGH, Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, beigefügt als Anlage 4a; BGH, Beschluss vom 25.11.2006, Aktenzeichen 1 BGs 184/06, bei Beck Online, beigefügt als Anlage 4b; BGH, Beschluss vom 21.2.2006, Aktenzeichen 3 BGs 31/06 = StV 2007, 60 ff., beigefügt als Anlage 4c.

ne taugliche Ermächtigung in der Strafprozessordnung gibt[70] und dafür überwiegend Zustimmung erhalten[71].

Geprüft – und als mögliche Rechtsgrundlagen abgelehnt – wurden § 102 StPO, § 100 a StPO, § 100 c StPO, § 100 f Abs. 1 Nr. 2 StPO und § 161 StPO. Auch eine **Kombination aus bereits vorhandenen Ermächtigungen** sei rechtlich **unzulässig**.[72] Insbesondere die §§ 102 ff. StPO schieden aus, weil es sich bei einer **Durchsuchung** in diesem Sinne regelmäßig um eine **offene Maßnahme** gegenüber dem Betroffenen handeln müsse.[73]

4. Anforderungen an eine mögliche Eingriffsgrundlage

4.1. Qualität der Rechtsgrundlage

Aufgrund der Eingriffsintensität und der möglichen Betroffenheit von Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG ist eine **qualifizierte Eingriffsgrundlage** zu fordern, die sich inhaltlich an den engen Vorgaben der §§ 100a, 100b StPO[74] zu orientieren hätte.

Die Verfassungsgerichte haben in verschiedenen Entscheidungen die Anforderungen an die **Verfassungsmäßigkeit heimlicher Ermittlungsmaßnahmen** konkretisiert[75] und fordern insbesondere die Beachtung

- des Grundsatzes der Verhältnismäßigkeit,
- des Schutzes des Kernbereichs privater Lebensgestaltung,
- des Bestimmtheitsgrundsatzes.

4.2. Anforderungen an den Inhalt einer Eingriffsgrundlage

Der **Grundsatz der Verhältnismäßigkeit** verlangt, dass eine gesetzliche Regelung der Online-Durchsuchung **geeignet**, **erforderlich** und **angemessen** sein muss.[76]

---

70 BGH, Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, beigefügt als Anlage 4a; so zuvor schon BGH, Beschluss vom 25.11.2006, Aktenzeichen 1 BGs 184/06, beigefügt als Anlage 4b.

71 Hornung, CR 2007, 144 (144); Jahn/Kudlich, JR 2007, 57 (58); Leipold, NJW-Spezial 2007, 135 (136); Gercke, CR 2007, 245 (251); Bär, MMR 2007, 175 (177); schon zuvor in diesem Sinne, Böckenförde, S. 240; a.A. Hofmann, NStZ 2005, 121 (123); Graf, DRiZ 1999, 281 (285), mit dem Argument, dass eine heimliche Durchsuchung erheblich weniger beeinträchtigend sei, weil der Geschäftsbetrieb oder der häusliche Bereich nicht fühlbar gestört würden.

72 BGH, Beschluss vom 31.1.2007, Aktenzeichen StB 18/06, Rn. 22, beigefügt als Anlage 4a.

73 In diesem Sinne auch Bär, MMR 2007, 175 (176); außerdem Rückschluss aus BVerfG, NJW 2006, 976 (981), beigefügt als Anlage 3.

74 Vgl. Gesetzentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drs. 275/07, S. 5 ff., Begründung S. 84 ff.

75 Vgl. BVerfGE 109, 279 ff. = NJW 2004, 999 ff.; SächsverfGH, NVwZ 2005, 1310 ff.; VerfGH Rheinland-Pfalz, Urteil vom 29.1.2007, Aktenzeichen VGH B 1/06, www.verfgh.justiz.rpl.de; ausführlich hierzu Puschke/Singelnstein, NJW 2005, 3534 ff., beigefügt als Anlage 6; Warntjen, KJ 2005, 276 ff. (m.w.N. in Fn. 6).

76 Definitionen bei Sommermann, in: v. Mangoldt/Klein/Starck, GG, Art. 20 Abs. 3, Rn. 314, m.w.N.

W

Diesbezüglich hat Justizministerin Brigitte Zypries eine intensive Prüfung angemahnt:

> *„Es reicht nicht zu sagen: Wir brauchen das dringend. Ich will wissen, was genau und wofür sie etwas brauchen. Detailliert. (…) Erst müssen mich die Sicherheitsbehörden überzeugen, dass eine Online-Durchsuchung erforderlich und technisch möglich ist.“*[77]

Weiterhin ist bei heimlichen Beobachtungen ein **unantastbarer Kernbereich privater Lebensgestaltung** zu wahren.[78] 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.[79] Dementsprechend hat der Staat bereits im Gesetz **Schutzmechanismen** zu installieren, die eine Verletzung ausschließen.[80]

Schließlich soll der **Bestimmtheitsgrundsatz** sicherstellen, dass der betroffene **Bürger** sich auf mögliche belastende Maßnahmen einstellen kann, die **Verwaltung** steuernde und begrenzende Handlungsmaßstäbe vorfindet und die **Gerichte** die Rechtskontrolle wirksam durchführen können. Der **Anlass, der Zweck und die Grenzen des Eingriffs müssen** in der Ermächtigung **bereichsspezifisch, präzise und normenklar festgelegt werden**. Bei Ermächtigungen zu Überwachungsmaßnahmen verlangt das Bestimmtheitsgebot, dass die betroffene Person erkennen kann, bei welchen Anlässen und unter welchen Voraussetzungen ein Verhalten mit dem Risiko der Überwachung verbunden ist.[81]

[redacted]

---

77 Interview mit der Bundesjustizministerin, in: Die Welt vom 7.5.2007; ähnlich schon in einer Rede beim Europäischen Polizeikongress am 13.2.2007, www.bmj.bund.de; kritisch gegenüber der Wirksamkeit Buermeyer, HRR-Strafrecht 2007, 154 (164 ff.), beigefügt als Anlage 1; zu möglichen Nachteilen gegenüber herkömmlichen Ermittlungsmaßnahmen vgl. Gercke, CR 2007, 245 (246 ff.); siehe auch die Debatte im Landtag Rheinland-Pfalz, Plenarprotokoll 15/18, S. 980 – 985; für die Notwendigkeit hingegen ausdrücklich Hofmann, NStZ 2005, 121 (125).

78 Vgl. den Gesetzentwurf der Bundesregierung zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drs. 275/07, S. 1 und 85.

79 BVerfG, NJW 2004, 999 (1002).

80 Zu den Anforderungen siehe BVerfG, NJW 2004, 999 (1002 ff.); Warntjen, KJ 2005, 276 ff.; Rux, JZ 2007, 285 (291), beigefügt als Anlage 2.

81 BVerfGE 110, 33 (53 f.); BVerfGE 113, 348 (375 f.).

5. Literaturverzeichnis

- **Bär**, Wolfgang, Anmerkung zu BGH, Beschluss vom 25.11.2006, 1 BGs 184/2006, Multimedia und Recht 2007, S. 175 – 177 (zit.: Bär, MMR 2007).
- **Baum**, Gehart; **Reiter**, Julius Friedrich; **Schantz**, Peter, Antragsschrift der Verfassungsbeschwerde vom 1.3.2007 gegen das Verfassungsschutzgesetz Nordrhein-Westfalen, S. 1 – 52, abrufbar unter http://www.hrr-strafrecht.de/hrr/doku/2007/001/index.php (zit.: Baum/Reiter/Schantz).
- **Beulke**, Werner, Anmerkung zu BGH, Beschluss vom 21.2.2006, Aktenzeichen 3 BGs 31/06, StV 2007, S. 63 – 65 (zit.: Beulke, StV 2007).
- **Böckenförde**, Thomas, Die Ermittlung im Netz, 2003 (zit. Böckenförde).
- **Buermeyer**, Ulf, Die „Online-Durchsuchung". Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, in: HRR-Strafrecht (Internetzeitung für Strafrecht), www.hrr-strafrecht.de, Ausgabe 4/2007, S. 154 – 166 (zit.: Buermeyer, HRR-Strafrecht 2007).
- **Gercke**, Marco, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, Computer und Recht 2007, S. 245 – 253 (zit.: Gercke, CR 2007).
- **Germann**, Michael, Gefahrenabwehr und Strafverfolgung im Internet, 2000 (zit.: Germann).
- **Graf**, Jürgen, P., Internet: Straftaten und Strafverfolgung, DRiZ 1999, S. 281 – 286 (zit.: Graf, DRiZ).
- **Gusy**, Christoph, Auswirkungen des Lauschangriffsurteils außerhalb der strafpozessualen Wohnungsüberwachung, in: **Schaar**, Peter (Hrsg.), Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung, 2004, S. 35 – 59 (zit.: Gusy, Auswirkungen des Lauschangriffsurteils).
- **ders.**, in: **von Mangoldt**, Hermann; **Klein**, Friedrich; **Starck**, Christian (Hrsg.), Kommentar zum Grundgesetz, Band 1, 5. Auflage 2005 (zit.: Gusy, in: v. Mangoldt/Klein/Starck, GG).
- **ders.**, Stellungnahme 14/629 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 9 (zit.: Gusy).
- **Hofmann**, Manfred, Die Online-Durchsuchung – staatliches „Hacken" oder zulässige Ermittlungsmaßnahme, NStZ 2005, S. 121 – 125 (zit.: Hofmann, NStZ 2005).
- **Hornung**, Gerrit, Rechtswidrigkeit heimlicher Computerausforschung, Computer und Recht 2007, S. 144 – 145 (zit.: Hornung, CR 2007).
- **Huster**, Stefan, Stellungnahme 14/641 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 9 (zit.: Huster).
- **Jahn**, Matthias, **Kudlich**, Hans, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57 – 61 (zit.: Jahn/Kudlich, JR 2007).

- **Kaufmann**, Noogie C., Anmerkung zu BGH, Beschluss vom 25.11.2006, 1 BGs 184/2006, Multimedia und Recht 2007, S. 175 (zit.: Kaufmann, MMR 2007).
- **Kutscha**, Martin, Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169 – 1172 (zit: Kutscha, NJW 2007).
- **Leipold**, Klaus, Die Online-Durchsuchung, NJW-Spezial 2007, S. 135 – 136 (zit.Leipold, NJW-Spezial 2007).
- **Lorentz**, Jürgen, Stellungnahme 14/639 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 9 (zit.: Lorentz).
- **Löwer**, Wolfgang, in: **v. Münch**, Ingo; **Kunig**, Philip (Hrsg.), Grundgesetz-Kommentar, Band 1, 5. Auflage 2000 (zit.: Löwer, in: v. Münch/Kunig).
- **Puschke**, Jens; **Singelnstein**, Tobias, Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, S. 3534 -3538 (zit.: Puschke/Singelnstein, NJW 2005).
- **Roggan**, Frederik, Antragsschrift der Verfassungsbeschwerde vom 9.2.2007 gegen das Verfassungsschutzgesetz Nordrhein-Westfalen, S. 1 – 37, abrufbar unter http://www.hrr-strafrecht.de/hrr/doku/2007/001/index.php (zit.: Roggan).
- **Roth, Wolfgang,** Stellungnahme 14/645 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 26. (zit.: Roth).
- **Rux**, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 185 – 295 (zit.: Rux, JZ 2007).
- **Sachs**, Michael, Grundgesetz, Kommentar, 3. Auflage 2003 (zit.: Sachs, GG).
- **Schwarz, Kyrill,** Stellungnahme 14/650 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 12 (zit.: Schwarz).
- **Störing**, Marc, Zum Umfang von Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung, Computer und Recth 2007, S. 392 – 393 (zit.: Störing, CR 2007).
- **Sokol**, Bettina, Stellungnahme 14/625 zum Gesetz der Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen (VSG-E), Anhörung am 19.10.2006, www.landtag.nrw.de, S. 1 – 9 (zit.: Sokol).
- **Sommermann, Karl-Peter, in: von Mangoldt**, Hermann; **Klein**, Friedrich; **Starck**, Christian (Hrsg.), Kommentar zum Grundgesetz, Band 2, 5. Auflage 2005 (zit.: Sommermann, in: v. Mangoldt/Klein/Starck, GG).
- **Warntjen**, Maximilian, Der Kernbereich privater Lebensgestaltung und die Telekommunikationsüberwachung gemäß § 100a StPO, Kritische Justiz 2005, S. 276 – 286 (zit.: Warntjen, KJ 2005).
- **Wohlfahrth**, Jürgen, Rechtliche und tatsächliche Aspekte der Videoüberwachung im öffentlichen Raum, Zeitschrift für Landes- und Kommunalrecht 2007, S. 54 – 59. (zit.: Wohlfarth, LKRZ 2007).
- **Zöller**, Mark, Möglichkeiten und Grenzen polizeilicher Videoüberwachung, NVwZ 2005, S. 1235 – 1241 (zit.: Zöller, NVwZ 2005).

W

6. Anlagenverzeichnis

- **Buermeyer**, Ulf, Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, in: HRR-Strafrecht 4/2007 (Internetzeitung für Strafrecht), S. 154 – 166.

  - beigefügt als Anlage 1 -

- **Rux**, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 185 – 295.

  - beigefügt als Anlage 2 -

- **Bundesverfassungsgericht** zur Beschlagnahme gespeicherter Telekommunikationsdaten, Urteil vom 2.3.2006, Aktenzeichen 2 BvR 2099/04, NJW 2006, S. 976 – 984.

  - beigefügt als Anlage 3 -

- **Bundesgerichtshof zur „verdeckten Online-Untersuchung“**

  - Beschluss vom 31.1.2007, Aktenzeichen StB 18/06.

    - beigefügt als Anlage 4a -

  - BGH, Beschluss vom 25.11.2006, Aktenzeichen 1 BGs 184/06.

    - beigefügt als Anlage 4b -

  - BGH, Beschluss vom 21.2.2006, Aktenzeichen 3 BGs 31/06.

    - beigefügt als Anlage 4c -

- **Überblick über maßgebliche Rechtsgrundlagen**, Auszüge aus den in der Diskussion stehenden Gesetzen.

  - beigefügt als Anlage 5 -

- **Puschke**, Jens; **Singelnstein**, Tobias, Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, S. 3534 – 3538 (zit.: Puschke/Singelnstein, NJW 2005).

  - beigefügt als Anlage 6 -