

Constantin Eikel

„Online-Durchsuchungen“ durch Polizei-
und Sicherheitsbehörden im Spiegel des
Verfassungsrechts

Studienarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Thema
„Online-Durchsuchungen“ durch Polizei- und
Sicherheitsbehörden im Spiegel des
Verfassungsrechts

Inhaltsverzeichnis

Inhaltsverzeichnis	I
Literaturverzeichnis	III
A. Begriff und Arten der Online-Durchsuchung	1
Offenkundigkeit	1
1. Datenspiegelung.....	1
2. Daten-Monitoring	2
3. Kompletzzugriff.....	2
B. Bisherige Rechtsgrundlagen.....	2
1. Strafprozessordnung	2
a. §161 StPO	2
b. §110a StPO	3
c. §100a StPO.....	3
d. §§102, 103 StPO	4
2. Urteile	5
a. Überwachung einer Mailbox, 31.07.1995.....	5
b. Telekommunikationsüberwachung, 14.07.1999	5
c. Telekommunikationsüberwachung, 27.07.2005	5
d. Zulässigkeit einer heimlichen Online-Durchsuchung eines Computers, 21.02.2006... 6	
e. Unzulässigkeit der Durchsuchung eines Personalcomputers, 25.11.2006.....	6
f. Unzulässigkeit der „verdeckten Online-Durchsuchung“, 31.01.2007.....	6
C. Verfassungsrechtliche Grenzen	7
I. Telekommunikationsfreiheit, Art. 10 I GG	7
1. Allgemeine Bedeutung.....	7
2. Rechtfertigung von Beeinträchtigungen	8
II. Unverletzlichkeit der Wohnung, Art. 13 GG	10
1. Allgemeine Bedeutung.....	10
a. <i>Private Wohnungen</i>	10
b. <i>Geschäftsräume</i>	12
2. Rechtfertigung von Beeinträchtigungen	13
a. <i>Besonders schwere Straftat, Art. 13 III GG</i>	13
b. <i>Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, Art. 13 IV GG</i>	13
c. <i>Unterrichtungspflicht des Bundes, Art. 13 VI GG</i>	14
3. Systemarten.....	14
a. <i>Intern</i>	14

<i>b. Extern</i>	14
<i>c. Mobil</i>	16
4. Kritik.....	16
III. Informationelle Selbstbestimmung, Art. 2 I i.V.m. Art 1 I GG.....	17
1. Grundsatz und Herleitung.....	17
2. Anwendbarkeit.....	18
3. Rechtfertigung von Beeinträchtigungen.....	18
D. Notwendigkeit neuer Ermächtigungsgrundlagen - Fazit.....	19

Literaturverzeichnis

- Battis, Ulrich*, Schutz der Gewerberäume durch GG Art 13 und Wirtschafts-, Arbeits- und Steueraufsicht, JuS 1973, S. 25 – 30.
- Beulke, Werner, u. Meininghaus, Florian*, Verdeckte Durchsuchung eines Computers mittels heimlich installiertem Computerprogramm, StV 2007, S. 63 – 65.
- Bizer, Johann*, Gegen die Online-Durchsuchung, Datenschutz und Datensicherung 2007, S. 640.
- Böckenförde, Thomas*, Die Ermittlung im Netz, 1. Aufl. 2003, Tübingen.
- Buermeyer, Ulf*, Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme, HRRS 2007, S. 154 – 166.
- Dolzer Rudolf (Gesamthrg.), u. Vogel, Klaus (Mithrg.)*, Bonner Kommentar zum Grundgesetz, Loseblattsammlung, 15 Bände: Band 3, 83. Aktualisierung, 1991 (Stand: 131. Aktualisierung September 2007), Heidelberg.
- Dreier, Horst (Hrsg.)*, Grundgesetz-Kommentar, 3 Bände: Bd. 1: 2. Aufl. 2004, Tübingen.
- Eisenberg, Ulrich*, Straf(verfahrens-) rechtliche Maßnahmen gegenüber „Organisiertem Verbrechen“, NJW 1993, S. 1033 – 1039.
- Gusy, Christoph*, Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, S. 89 – 96.
- Hoffmann, Manfred*, Die Online-Durchsuchung – staatliches „Hacken“ oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121 – 125.
- Hornung, Gerrit*, Erwiderung zu „Die Festplatte als Wohnung?“, JZ 2007, S. 828 – 831.
- Huber, Bertold*, Trojaner mit Schlapphut – Heimliche Online-Durchsuchung nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, NVwZ 2007, S. 880 – 884.
- Hund, Horst*, Der Einsatz technischer Mittel in Wohnungen, ZRP 1995, S. 334 – 338.
- Jarass, Hans, u. Pieroth, Bodo*, Grundgesetz für die Bundesrepublik Deutschland Kommentar, 9. Aufl. 2007, München.
- Kudlich, Hans, u. Jahn, Matthias*, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, JR 2007, S. 57 – 61.
- Kutscha, Martin*, Verdeckte „Online-Durchsuchung“ und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169 – 1172.
- Maunz, Theodor, u. Dürig, Günter, herausgegeben von Herzog, Roman, Scholz, Rupert, Herdegen, Matthias u., Klein, Hans*, Grundgesetz Kommentar, Loseblattsammlung, 6 Bände, Band 1, 50. Aktualisierung, 2007, München.
- Meyer-Göfner, Lutz*, Strafprozessordnung, 50. Auflage 2007, München.
- Park, Tido*, Handbuch Durchsuchung und Beschlagnahme, 1. Aufl. 2002, München.
- Pieroth, Bodo u. Schlink, Bernhard*, Grundrechte Staatsrecht II, 22. Aufl. 2006, München.

Rux, Johannes, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 286 – 295.

Schaar, Peter, u. Landwehr, Sebastian, Anmerkung zum Beschluss des BGH vom 31.1.2007, K&R 2007, S. 202 – 205.

Valerius, Brian, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, 1. Aufl. 2004, Berlin.

Valerius, Brian, Ermittlungsmaßnahmen im Internet, JR 2007, S. 275 – 280.

v. Mangoldt, Hermann(Hrsg.), Klein, Friedrich(Hrsg.), u. Starck, Christian (Hrsg.), Kommentar zum Grundgesetz, 3 Bände: Bd. 1: 5. Aufl. 2005, München.

A. Begriff und Arten der Online-Durchsuchung

Um Online-Durchsuchungen im Spiegel des Verfassungsrechts beurteilen zu können, ist es zunächst notwendig, den Begriff der Online-Durchsuchung genauer zu definieren, und etwaige verschiedene Arten klar abzugrenzen. Laut dem Generalbundesanwalt ist damit die „Durchsuchung des [...] Personalcomputers/Laptops, insbesondere der auf der Festplatte und im Arbeitsspeicher abgelegten Dateien [...]“¹ gemeint. Hierbei handelt es sich aber nicht um einen Sonderfall der Durchsuchung gem. §§102ff. StPO². Viel mehr wird „dabei [...] ein Computerprogramm von außen auf dem Zielrechner installiert, das sodann die in den Speichermedien [...] eines Rechners befindlichen Daten zur Durchsicht an die Ermittlungsbehörden überträgt, sobald der Benutzer des Rechners eine Verbindung mit dem Internet herstellt.“³ Grundsätzlich geht es also um die Durchsuchung des Computers.

Offenkundigkeit

Jegliche Art der Online-Durchsuchung kann offen oder verdeckt stattfinden.⁴ Der Fall der offenen Online-Durchsuchung kann wohl aber vernachlässigt werden, da er kaum bis gar nicht zur Anwendung kommt. Bei einer offenen Online-Durchsuchung hätte der Verdächtige genügend Zeit etwaige Daten zu löschen oder unbrauchbar zu machen, da auf Grund der heutigen technischen Möglichkeiten eine sofortige Datensicherung nicht möglich ist. Dadurch, dass der Verdächtige keine Kenntnis von der Online-Durchsuchung erlangt, wird auch die Verschüttung anderer Ermittlungsansätze verhindert⁵. Auf Grund dessen wird im Folgenden grundsätzlich von einer verdeckten Online-Durchsuchung ausgegangen. Diese kann aber auf verschiedene Arten erfolgen.

1. Datenspiegelung

Bei der Datenspiegelung handelt es sich um einen einmaligen Zugriff auf die Daten des Zielcomputers. Dieser Zugriff kann in der Suche nach bestimmten Dateien oder in Form einer kompletten Kopie des gesamten Datensystems (Spiegelung) liegen. Diese Art der Online-Durchsuchung „kommt der klassischen Beschlagnahme und Auswertung eines Rechners am nächsten: Hier wie dort steht der (sic!) Ermittlern eine Momentaufnahme

¹ BGH, JZ 2007, S. 796 (798).

² *Kutscha*, Verdeckte „Online-Durchsuchung und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169.

³ *Valerius*, Ermittlungsmaßnahmen im Internet, JR 2007, S. 275 (276).

⁴ *Rux*, Ausforschung privater Rechner durch die Polizei- und Sicherheitsbehörden, JZ 2007, S. 285 (286).

⁵ *Hofmann*, Die Online-Durchsuchung – staatliches „Hacken“ oder zulässige Ermittlungsmaßnahme?, NStZ 2005, S. 121.

der EDV-Anlage zur Verfügung.“⁶ Nach der Datenspiegelung ist die Online-Durchsuchung des Zielcomputers beendet.

2. Daten-Monitoring

Das Daten-Monitoring zeichnet sich dadurch aus, dass zunächst auch eine Datenspiegelung vorgenommen wird, allerdings wird danach der Zugriff nicht beendet, sondern jede weitere Veränderung im Dateisystem mitgeschrieben – womit der Betroffene Dateien zwar löschen kann, diese aber dennoch für die Ermittlungsbehörden erhalten bleiben. Insoweit verliert der Betroffene die Hoheit über seine Dateien.⁷ Hierbei handelt es sich somit um eine auf einen längeren Zeitraum angelegte Online-Durchsuchung.

3. Komplettzugriff

Beim Komplettzugriff handelt es sich um eine Realüberwachung. Sie kommt einer totalen Observation gleich, da jeder Tastaturanschlag, jede Mausbewegung sowie Ausgabe am Bildschirm gespeichert wird, und somit nachvollziehbar ist. Den Ermittlungsbehörden steht jede Funktion des Computers offen, die auch der eigentliche Benutzer in Anspruch nehmen kann.⁸ Diese Art der Online-Durchsuchung ist die wohl intensivste. Der Komplettzugriff zeichnet sich wie das Daten-Monitoring dadurch aus, dass er auf Dauer angelegt ist.

B. Bisherige Rechtsgrundlagen

Im Rahmen dieser Arbeit bleibt zu prüfen, ob die bisherigen Rechtsgrundlagen den verfassungsrechtlichen Ansprüchen, wie im Teil C. dargestellt, genügen.

1. Strafprozessordnung

Da die technische Entwicklung nicht vorhersehbar ist, und der Gesetzgeber oft nur auf bereits vorhandene Sachverhalte reagiert, mangelt es momentan an einer ausdrücklichen Ermächtigungsgrundlage für Online-Durchsuchungen in der StPO. Fraglich ist aber, ob eine bereits vorhandene Norm als Ermächtigungsgrundlage für die Online-Durchsuchung analog angewandt werden kann.

a. §161 StPO

⁶ *Buermeyer*, Die „Online-Durchsuchung“. Technischer Hintergrund des verdeckten hoheitlichen Zugriffs auf Computersysteme“, HRRS 2007, S. 154 (160).

⁷ *Buermeyer*, (Fn. 6), S. 154 (161).

⁸ *Buermeyer*, (Fn. 6), S. 154 (162).

Der §161 StPO stellt eine Ermittlungsgeneralklausel dar.⁹ Er deckt nur solche Ermittlungen ab, die eine geringere Grundrechtseingriffsintensität aufweisen.¹⁰ Alle Formen der Online-Durchsuchung können allerdings die Grundrechte aus Art. 10, 13 GG tangieren¹¹, und berühren jedenfalls das Recht auf informationelle Selbstbestimmung¹². Ebenfalls berührt die Online-Durchsuchung die geschützte Privatsphäre aus Art. 2 I GG, so dass ein Rückgriff auf die Ermittlungsgeneralklausel bereits deshalb ausscheidet.¹³

b. §110a StPO

Denkbar wäre auch eine Legitimierung der Online-Durchsuchung über den Verdeckten Ermittler des §§110a, 110b StPO. Allerdings beschränkt der §110c S. 1 StPO die Rechte des Verdeckten Ermittlers auf den Zutritt der Wohnung unter Verwendung der Legende. „Ebenso wenig wie der Verdeckte Ermittler eine ‚klassische‘ Durchsuchung ohne die Voraussetzungen der §§102, 103, 105 StPO vornehmen dürfte, ist dies ohne spezialgesetzliche Bezugsnorm bei der Online-Durchsuchung möglich [...]“¹⁴

c. §100a StPO

Der §100a StPO ermöglicht den Ermittlungsbehörden unter bestimmten Voraussetzungen die Überwachung der sonst gem. Art. 10. I GG geschützten Telekommunikation (auf den Schutzbereich wird später einzugehen sein). In der Mailbox Entscheidung des BGH vom 31.07.1995¹⁵ stellt der Ermittlungsrichter fest: „§100a StPO läßt die Überwachung des Fernmeldeverkehrs nicht nur in den herkömmlichen Formen des Telefonierens und Fernschreibens, sondern jeglicher Art der Nachrichtenübermittlung zu.“¹⁶ In besagter Entscheidung wird festgestellt, dass „auch der heimliche Zugriff auf die in den Mailboxen der betroffenen Anschlußinhaber gespeicherten Daten [...] im Rahmen der Telefonüberwachung grundsätzlich zulässig“¹⁷ ist. Fraglich ist nun, ob darunter auch die Online-Durchsuchung subsumiert werden kann. Dies hat das BVerfG in einer früheren Entscheidung bereits bejaht, denn der Begriff der Fernmeldeanlage sei „vom Gesetzgeber bewußt offengehalten worden für neue, seinerzeit noch nicht bekannte Techniken der Nachrichtenübertragung.“¹⁸ Eine Anwendung auf die Online-Durchsuchung ist ebenfalls insofern nahe liegend, als dass ein Zugriff wie bei der Telekommunikation nur erfolgen

⁹ Meyer-Goßner, StPO, 50. Aufl., §161 Rn. 1.

¹⁰ Meyer-Goßner, (Fn. 9), §161 Rn. 1.

¹¹ Hofmann, (Fn. 5), S. 121.

¹² BVerfGE, 65, 1ff.

¹³ Böckenförde, Die Ermittlung im Netz, S. 240.

¹⁴ Hofmann, (Fn. 5), S. 121 (122).

¹⁵ BGH, NSTZ 1997, S. 247.

¹⁶ BGH, (Fn. 15), S. 247.

¹⁷ BGH, (Fn. 15), S. 247 (248).

¹⁸ BVerfGE 46, S. 120 (142).

kann, wenn sie gerade aktiv benutzt wird, der Verdächtige also „online“ ist.¹⁹ Allerdings würde bei einer Online-Durchsuchung nicht nur der aktuell in das Internet führende Datenstrom angezapft, sondern durch die offene Leitung auf Daten innerhalb des Computers zugegriffen, die der Verdächtige nicht willentlich in den „Datenkanal“ bringen wollte. Die Übertragung eben dieser Daten würde also durch die Ermittlungsbehörden ausgelöst, und nicht durch den Verdächtigen selbst, er hat praktisch gesprochen „nur die Tür geöffnet“. Dass bei einer Datenübertragung, die durch die Ermittlungsbehörden ausgelöst wurde, nicht mehr von einer Überwachung der Telekommunikation i.S.d. §100a StPO gesprochen werden kann, hat der 2. Strafsenat des BGH in seiner Entscheidung vom 14.03.2003 festgestellt.²⁰ Das BVerfG hat in der Bargatzky-Entscheidung ebenfalls festgestellt, dass das Abrufen von E-Mails vom Computer des Verdächtigen nicht den Begriff der Telekommunikation des §100a StPO erfüllt.²¹ Ein Rückgriff auf den §100a StPO als Ermächtigungsgrundlage für Online-Durchsuchungen ist damit ausgeschlossen

d. §§102, 103 StPO

Die Anwendung der §§102, 103 StPO auf die Online-Durchsuchung liegt insofern nahe, als dass sie die Durchsuchung beim Verdächtigen oder bei anderen Personen regeln. Ob diese Normen als Ermächtigungsgrundlage herangezogen werden können, war längst umstritten. Eine verbreitete Meinung lehnte dies mit der Begründung ab, dass jegliche Durchsuchung als offene Maßnahme durchzuführen sei, und sich durch die physische Anwesenheit der Ermittlungsbeamten am Ort der Durchsuchung auszeichne, was sich aus der Gesamtheit der Durchsuchungsvorschriften der §§102 bis 110 StPO ergebe.²² Andere Auffassungen argumentieren mit dem strafrechtlichen Durchsuchungsbegriff der durch das „ziel- und zweckgerichtete Suchen staatlicher Organe [...] nach Verborgenen“²³ in einem bestimmten abgrenzbaren Bereich oder Objekt gekennzeichnet wird. Sie ist also gerade nicht durch die zwingende Offenheit der Durchsuchungsmaßnahme ausgezeichnet.²⁴ Der Ermittlungsrichter des BGH ließ §§102, 103 StPO in seiner Entscheidung vom 21.02.2006 als Ermächtigungsgrundlage ausreichen²⁵, was aber am 25.11.2006 vom BGH bereits wieder verneint wurde.²⁶ In letztgenannter Entscheidung wurde als Argument angeführt, dass die Durchsuchung gem. §102 StPO ein körperlicher, nicht ein elektronischer Vorgang, und im Grunde auf Offenheit angelegt sei. Die Relativierung

¹⁹ Münch-Komm-Graf, §212a Rn. 64.

²⁰ BGH, NJW 2003, S. 2034 (2035).

²¹ BVerfG NJW 2006, S. 976 (980); m. Anm. Kudlich, Die strafprozessuale Zulässigkeit der Online-Durchsuchung, S. 57 (61).

²² Bär CR 1995, 489, 494; Zöllner GA 2000, 563, 572, 573, Eisenberg NJW 1993, 1003, 1038; zusammenfassend Hofmann (Fn. 5), S. 121 (123).

²³ Park, Handbuch Durchsuchung und Beschlagnahme, 2002, Rn. 30.

²⁴ Hofmann, (Fn. 5), S. 121 (123).

²⁵ BGH, Beschl. v. 21.2.2006 – 3BGs 31/06.

²⁶ BGH, Beschl. v. 25.11.2006 – 1 BGs 184/06.

„wenn möglich“ des §106 I StPO in Bezug auf die Anwesenheit der Zeugen sei keine ermittlungstaktische Erwägung, sondern hätte ausschließlich tatsächliche Schwierigkeiten im Auge, also die faktische Unmöglichkeit den Inhaber hinzuzuziehen. Eine Online-Durchsuchung auf Grundlage der §§102, 103 StPO ist somit ausgeschlossen.

2. Urteile

Um die Online-Durchsuchung im Spiegel des Verfassungsrechts zu betrachten, ist es sinnvoll einen kurzen historischen Abriss über die Entscheidungen der höchstrichterlichen Rechtsprechung zu geben. Die Unzulänglichkeit der bisher genannten Normen im Hinblick auf die Online-Durchsuchung ist zwar bereits festgestellt, dennoch ist die Entwicklung bis zur aktuellen Rechtsprechung ein interessanter Prozess. Allerdings gibt es für das junge Problem der Online-Durchsuchung kaum Entscheidungen. Jedoch lässt sich das generelle Problem der technischen Überwachung beurteilen, und durch die Nähe der Telekommunikationsüberwachung zur Online-Durchsuchung eine Entwicklung der Rechtsprechung festmachen.

a. Überwachung einer Mailbox, 31.07.1995

In der bereits genannten „Mailbox“²⁷ Entscheidung ließ der Ermittlungsrichter des BGH §100a StPO für jegliche Art der Nachrichtenübermittlung genügen. Fraglich ist, ob der Ermittlungsrichter die Online-Durchsuchung mit diesem Urteil schon im Blick hatte, da eben jene erst eine Entwicklung der letzten Jahre ist.

b. Telekommunikationsüberwachung, 14.07.1999

In der Entscheidung „Telekommunikationsüberwachung“²⁸ hatte das BVerfG über die Vereinbarkeit des aus Art. 10 GG resultierende Recht auf Telekommunikationsfreiheit und der Überwachung, Aufzeichnung und Auswertung des Telekommunikationsverkehrs zu entscheiden. Auf den gesamten Schutzbereich wird später einzugehen sein, festzustellen ist aber, dass das BVerfG eben jenen Schutzbereich auch auf die Verarbeitung, Auswertung und Weitergabe der erhobenen Daten an andere Behörden anwendet, sich also jeder Vorgang mit den erhobenen Daten an den Grundrechten zu messen hat. Diese Feststellung der Weite des Schutzbereiches lässt sich wohl auch auf die Erhebung von Daten mittels der Online-Durchsuchung übertragen, so dass für eben jene die gleichen Grundsätze gelten werden.

c. Telekommunikationsüberwachung, 27.07.2005

²⁷ BGH, NSTZ 1997, S. 247.

²⁸ BVerfG, NJW 2000, S. 55.

In dieser gleich lautenden Entscheidung²⁹ hat das BVerfG die Entwicklung von Ermächtigungsgrundlagen durch die Länder gestoppt. Der Bundesgesetzgeber habe abschließend von seiner Gesetzgebungsbefugnis aus Art. 74 I Nr. 1 GG Gebrauch gemacht, die Verfolgung von Straftaten durch Maßnahmen der Telekommunikationsüberwachung zu regeln.³⁰ Es ist davon auszugehen, dass der Bundesgesetzgeber auch bei der Überwachung bzw. Durchsuchung im Rahmen der Online-Durchsuchung von seiner Gesetzgebungskompetenz Gebrauch machen wird (wenn man nicht bereits von einer ausreichenden Ermächtigungsgrundlage in der StPO ausgeht), da allein die Anwendung eines Landesgesetzes im Internet zu ungeahnten Schwierigkeiten führt.

d. Zulässigkeit einer heimlichen Online-Durchsuchung eines Computers, 21.02.2006

Der Ermittlungsrichter des BGH hat in dieser Entscheidung³¹ speziell für die Online-Durchsuchung festgestellt, dass §102 StPO eine heimliche Durchsuchung deckt, und dass der Begriff der Durchsuchung i.S.d. §§102ff. StPO auch die Suche nach elektronischen Daten meint. Ebenfalls wird allgemein festgestellt, dass eine Online-Durchsuchung zulässig ist, und ebenso kann es den Ermittlungsbehörden erlaubt werden „ein hierfür konzipiertes Computerprogramm von außen auf dem Computer des Beschuldigten zu installieren, um die auf den Speichermedien des Computers abgelegten Daten zu kopieren und zum Zwecke der Durchsicht an die Ermittlungsbehörden zu übertragen“³². Eine generelle Zulässigkeit der Online-Durchsuchung, und die spezielle Ermächtigung über §102 StPO, wurde in dieser Entscheidung somit bejaht.

e. Unzulässigkeit der Durchsuchung eines Personalcomputers, 25.11.2006

Nur neun Monate später stellte der Ermittlungsrichter des BGH jedoch fest, dass es sich bei einer heimlichen Online-Durchsuchung um „einen schwerwiegenden Eingriff in das den persönlichen Freiheitsrechten zuzuordnende Recht auf informationelle Selbstbestimmung“³³ handelt. Ebenfalls fehle es an der dafür notwendigen gesetzlichen Grundlage, entgegen der vorherigen Entscheidung.

In diesem relativ kurzen Zeitraum wurde nun also §102 StPO die Ermächtigung zur Online-Durchsuchung wieder abgesprochen.

f. Unzulässigkeit der „verdeckten Online-Durchsuchung“, 31.01.2007

²⁹ BVerfGE 113, S. 348.

³⁰ BVerfGE 113, S. 348.

³¹ BGH, Beschl. v. 21.2.2006 – 3BGs 31/06.

³² BGH, Beschl. v. 21.2.2006 – 3BGs 31/06.

³³ BGH, Beschl. v. 25.11.2006 – 1 BGs 184/06.

Der 3. Strafsenat des BGH erklärt die verdeckte Online-Durchsuchung in dieser Entscheidung mangels einer Ermächtigungsgrundlage für unzulässig³⁴. Er stellt insbesondere fest, und klärt damit den bisher herrschenden Streit, dass §102 StPO nicht als Ermächtigungsgrundlage ausreicht, und revidiert somit erneut das Urteil vom 21.02.2006. Anzumerken bleibt noch, „dass eine Ermächtigung auf Grundlage des §102 StPO selbst dann nicht in Betracht komme, wenn die hohen Eingriffsvoraussetzungen der §§100a, 100c StPO [...] gewahrt bleiben.“³⁵ Denn es sei „unzulässig, einzelne Elemente von Eingriffsermächtigungen zu kombinieren, um eine Grundlage für eine neue technisch mögliche Ermittlungsmaßnahme zu schaffen“³⁶ Der BGH hat somit die Zulässigkeit der Online-Durchsuchung nach geltendem Recht verneint.

Zusammenfassend ist zu sagen, dass in der anfänglichen Rechtsprechung die Online-Durchsuchung noch über bisherige Ermächtigungsgrundlagen erlaubt wurde. Mit andauernder Diskussion über eben diese Ermächtigungen, ist in den letzten Entscheidungen aber einhellig festgestellt worden, dass die bisherigen Ermächtigungsgrundlagen für eine verdeckte Online-Durchsuchung nicht ausreichen (dass aber nur diese verdeckte Durchsuchung Erfolg verspricht, wurde bereits erläutert). Um also das Mittel der Online-Durchsuchung den Ermittlungsbehörden zur Verfügung zu stellen, was durchaus sinnvoll erscheint, bedarf es neuer Ermächtigungsgrundlagen. Diese jedoch müssen derart gestaltet sein, dass die Grundrechte jedes einzelnen in Anbetracht der Intensität einer Online-Durchsuchung gewahrt bleiben.

Die Online-Durchsuchung ist nun also im Spiegel des Verfassungsrechts zu beleuchten.

C. Verfassungsrechtliche Grenzen

I. Telekommunikationsfreiheit, Art. 10 I GG

1. Allgemeine Bedeutung

Der Art. 10 GG gewährleistet Grundrechte auf Wahrung des Brief-, Post- und Fernmeldegeheimnisses.³⁷ Diese Grundrechte schützen die Vertraulichkeit individueller Kommunikation³⁸, wenn die Telekommunikationsteilnehmer auf Grund der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen sind³⁹ und auf Grund der Beteiligung Dritter an der Übermittlung besonders dem Zugriff Dritter

³⁴ BGH, JR 2007, S. 123.

³⁵ Valerius, (Fn. 3), S. 275 (277).

³⁶ BGH, JR 2007, S. 123 Rn. 22.

³⁷ *Hermes*, in: Dreier (Hrsg.), Grundgesetz-Kommentar, Bd. 1, 2. Aufl. 2004, Art. 10 Rn. 15.

³⁸ *Hermes*, (Fn. 37), Art. 10 Rn. 15.

³⁹ BVerfGE 85, 386 (396).

offen steht.⁴⁰ „Da durch diese Abhängigkeit von dem Kommunikationsmittler, [der] unerwünschter Zugriff von außen auf die zu überbringende Nachricht erleichtert wird, will das Fernmeldegeheimnis umfassend die Vertraulichkeit privater Kommunikationsvorgänge jeglichen Inhalts schützen“⁴¹.

Eine Besonderheit des Grundrechtes auf Telekommunikationsfreiheit gem. Art. 10 GG liegt darin, dass an der Telekommunikation immer mindestens zwei Personen teilnehmen. Somit sind mehrere Kommunikationsteilnehmer „neben- und miteinander grundrechtsberechtigt“⁴² und ihr Schutz gegenüber Dritten ist „zusammengespannt“⁴³. Dies hat zur Folge, dass der Staat bzw. die Ermittlungsbehörden diesen Schutzbereich nicht nur durch rechtfertigende Zustimmung eines Kommunikationsteilnehmers betreten dürfen, sondern der Zustimmung aller bedürfen, da sonst der Schutzbereich unterwandert würde.⁴⁴ Dies hat zur Folge, dass in Bezug auf die Online-Durchsuchung ein Eingriff nicht dadurch gerechtfertigt werden kann, dass etwa der Provider des Internetanschlusses, oder aber der Anbieter der E-Mail Box seine Zustimmung erteilt.

2. Rechtfertigung von Beeinträchtigungen

Ein Eingriff in das Brief-, Post- und Fernmeldegeheimnis ist gem. Art. 10 II S. 1 GG zulässig, wenn er auf Grund eines Gesetzes erfolgt.⁴⁵ Die Befugnis des Bundesnachrichtendienstes aus §§1, 3 G10, gewisse Telekommunikationsvorgänge zu kontrollieren, sei laut BVerfG bereits mit Art. 10 GG vereinbar.⁴⁶

Unter bestimmten Voraussetzungen erlaubt Art. 10 II S. 2 GG als Ausnahme hingegen, dass dem Betroffenen ein Grundrechtseingriff nicht offenbart werden muss, und dass ihm dagegen der Rechtsweg offen stünde.⁴⁷ Da die typische Online-Durchsuchung verdeckt stattfinden soll, um den Ermittlungserfolg nicht zu gefährden, muss sich jede dieser Durchsuchungen an den Anforderungen des Art. 10 II S. 2 GG messen. Eine solche verdeckte Durchsuchung ist also nur zu Zwecken des Verfassungs- und Staatsschutzes möglich. Dieser verdeckte Eingriff in die Grundrechte des Betroffenen ist von noch höherer Intensität als der offene, da ihm die Möglichkeit den Rechtsweg zu beschreiten verwehrt ist (durch schlichte Unwissenheit)⁴⁸. Das in Art. 19 IV festgelegte Recht auf die Beschreitung des Rechtsweges gegen Beeinträchtigungen durch die öffentliche Hand wird

⁴⁰ Gusy, Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, S. 89 (90).

⁴¹ Valerius, (Fn. 3), S. 275 (279).

⁴² Hermes, (Fn. 37), Art. 10 Rn. 17.

⁴³ BVerfGE 85, 386 (396, 398f.).

⁴⁴ Hermes, (Fn. 37), Art. 10 Rn. 17.

⁴⁵ Jarass, in Jarass/Pieroth (Hrsg.), Grundgesetz Kommentar, 9. Aufl. 2007, Art. 10 Rn. 16.

⁴⁶ BVerfG, NJW 2000, S. 55 (56).

⁴⁷ Hermes, (Fn. 37), Art. 10 Rn. 56.

⁴⁸ Hermes, (Fn. 37), Art. 10 Rn. 58.

in Art. 19 IV S. 3 GG insofern relativiert, als dass auf die nachträgliche Prüfung der Maßnahme (Art. 10 II S. 2 a.E. GG) verwiesen wird.

Fraglich bleibt, welche Zwecke des Verfassungs- und Staatsschutzes einen solchen Eingriff rechtfertigen. Das BVerfG hat diese ungenauen Begriffe in einer „verfassungskonformen Verfassungenauslegung“⁴⁹ genauer definiert⁵⁰:

Schutz bedeutet demnach Abwehr von Gefährdungen der Verfassungsordnung oder des Staates, wobei sich diese aus nachprüfbaren tatsächlichen Anhaltspunkten ergeben müssen⁵¹. Besondere Bedeutung müsse hierbei auf das Verhältnismäßigkeitsprinzip gelegt werden, dessen Beachtung die Formulierung des Art. 10 II 2 GG zulässt⁵². Ebenfalls müsse die den Rechtsweg ersetzende Kontrolle (Art. 10 II S. 2 a.E. GG) durch „von der Volksvertretung bestellte Organe und Hilfsorgane“ mindestens ebenso wirkungsvoll sein wie eine gerichtliche Kontrolle, auch, und gerade weil, der Betroffene keine Möglichkeit hat in diesem Ersatzverfahren mitzuwirken.⁵³ „Darüber hinaus müsse das Kontrollorgan über die notwendige Sach- und Rechtskunde verfügen, weisungsfrei sein, auf eine bestimmte Zeit fest berufen werden, über die Kompetenz verfügen, alle Organe, die mit der Vorbereitung, Entscheidung, Durchführung und Überwachung des Eingriffs befasst sind, und alle Maßnahmen dieser Organe zu überwachen, eine laufende Kontrolle auszuüben, über alle für die Entscheidung erheblichen Unterlagen des Falles verfügen und seine Kontrolle nach rechtlichen Maßstäben durchführen.“⁵⁴ Diese sehr spezifischen Anweisungen in Hinblick auf Art. 10 II S. 2 GG lassen sich nur dadurch erklären, dass in großen Teilen des Schrifttums und bei der vom Urteil abweichenden Meinung von drei Richtern⁵⁵ einhellig die Meinung besteht, dass die Verfassungsänderung des Art. 10 II S. 2 GG nicht mit Art. 79 III GG vereinbar ist. Durch diese Spezifikationen hat das BVerfG allerdings versucht, eine Vereinbarkeit von Art. 10 II S. GG mit Art. 79 III GG herbeizuführen. Der Streit über die Verfassungsmäßigkeit von Art. 10 GG kann an dieser Stelle aber ausgelassen werden, da sich eine mögliche Ermächtigungsgrundlage für Online-Durchsuchungen an geltendem Verfassungsrecht zu messen hat und nicht vorher zu klären ist, ob eben jene verfassungsrechtlichen Beschränkungen überhaupt verfassungsgemäß sind.

Festzuhalten ist also die Definition des Begriffes „Schutz“ und die Anforderungen an die nachträgliche Prüfung i.S.d. Art. 10 II S. 2 GG im Rahmen einer verdeckten Online-Durchsuchung. Eine solche Online-Durchsuchung wäre also nur zulässig, wenn

⁴⁹ *Hermes*, (Fn. 37), Art. 10 Rn. 60.

⁵⁰ BVerfGE 30, 1 (17ff).

⁵¹ BVerfGE 30, 1 (17ff).

⁵² BVerfGE 30, 1 (22); 67, 157 (173ff).

⁵³ BVerfGE 30, 1 (23).

⁵⁴ *Hermes*, (Fn. 37), Art. 10 Rn. 60.

⁵⁵ Sondervotum *Geller, v. Schlabrendorff, Rupp*, BVerfGE 30, 1 (33ff).

begründeter Verdacht dafür besteht, dass Gefahr für die Verfassungsordnung oder den Staat besteht, was wohl im häufigsten Anwendungsfall, der Bekämpfung des Terrorismus zu bejahren ist. Eine verdeckte Online-Durchsuchung zur Aufdeckung „minderer“ Straftaten ist somit nicht mit Art. 10 II S. 2 GG vereinbar. Ebenfalls müsste für jede Online-Durchsuchung das oben beschriebene nachträgliche Kontrollorgan angerufen werden, um den verwehrten direkten Rechtsweg zumindest nachträglich zu ersetzen. Selbst für die „mildeste“ Art der Online-Durchsuchung, die Datenspiegelung, bedürfte es dieser Schritte. Für die Anwendung der intensiveren Online-Durchsuchungen wird wohl eine noch höhere Messlatte angelegt werden müssen, um eine ungerechtfertigte Beeinträchtigung des Grundrechtes auf Telekommunikationsfreiheit i.S.d. Art. 10 GG zu verhindern.

II. Unverletzlichkeit der Wohnung, Art. 13 GG

1. Allgemeine Bedeutung

a. Private Wohnungen

Das Grundrecht der Unverletzlichkeit der Wohnung steht in engem Zusammenhang mit dem verfassungsrechtlichen Gebot der unbedingten Achtung der Privatsphäre des Bürgers.⁵⁶ Der Zweck des Grundrechtes der Unverletzlichkeit der Wohnung ist es, der räumlichen Privatsphäre eines jeden Grundrechtsberechtigten einen umfassenden Schutz zu garantieren und die Wohnung als Mittelpunkt freier Entfaltung zu schützen.⁵⁷ Der Begriff der Wohnung umschreibt einen Raum, durch den sich der Mensch der allg. Zugänglichkeit entzieht⁵⁸, wobei der Raum zum Aufenthalt von Menschen geeignet und bestimmt sein muss⁵⁹.

Fraglich ist, ob die Unverletzlichkeit der Wohnung auf die Online-Durchsuchung angewandt werden kann. Dies wurde durch den Ermittlungsrichter des BGH im Beschluss vom 21.02.2006 verneint, da der Raum der Wohnung weder betreten noch akustisch überwacht würde.⁶⁰ Dies scheint aber bedenklich, wenn man das Gegenstück zur Online-Durchsuchung in der „realen“ Welt betrachtet: „Ermittlungsbeamte dringen in die Wohnung des Betroffenen ein, überspielen die Daten des Rechners und verlassen die Wohnung wieder, ohne dass der Betroffene noch irgendeine andere Person etwas bemerken.“⁶¹ Dieses Vorgehen würde aber das Grundrecht des Art. 13 I GG verletzen, und wäre somit verfassungswidrig, da sich die Durchsuchung gerade durch ihren

⁵⁶ Gornig, in v. Mangoldt, Klein, Starck (Hrsg.), GG Kommentar, Bd. 1, 5. Aufl. 2005, Art. 13 Rn. 1.

⁵⁷ BVerfGE 18, S. 121 (131f).

⁵⁸ Gornig, in GG Kommentar (Fn. 56), Art. 13 Rn. 13.

⁵⁹ Herdegen, in Dolzer, Vogel (Hrsg.), Bonner Kommentar zum Grundgesetz, Art. 13 Rn. 28.

⁶⁰ BGH wistra 2007, 28 (29).

⁶¹ Valerius, (Fn. 3), S. 275 (279).

offenen Charakter auszeichnet.⁶² Fraglich ist nun, ob es nicht einen Wertungswiderspruch darstellt, wenn bei gleichem Ermittlungsziel, also dem Zugriff auf den Computer innerhalb einer Wohnung, nur auf Grund einer neuartigen Ermittlungsmaßnahme (der Online-Durchsuchung) eine Berührung des Schutzbereiches des Art. 13 GG ausgeschlossen ist⁶³. Die Beamten müssen die Wohnung nun zwar nicht mehr betreten, darauf darf aber nicht abzustellen sein. Denn nicht nur die möglichen Ermächtigungsgrundlagen der StPO müssen im Licht der neuen Technologie betrachtet werden, sondern auch die Schutzbereiche der Grundgesetze. „Eine fortgeschrittene Interpretation muss sich an dem sachlichen Schutzbereich des Grundrechts orientieren. Art. 13 I GG soll dem Einzelnen einen räumlichen Bereich der Privatsphäre sichern, auf die er zur Befriedigung elementarer Lebensbedürfnisse sowie zur Freiheit und Entfaltung seiner Persönlichkeit angewiesen ist.“⁶⁴ Dies bedeutet, dass jeder Betroffene auch selbst entscheiden können muss, welche Informationen er preisgeben will, und welche nicht. „Art. 13 GG schützt auch gegen die ungewollte informationelle Erhebung von [...] Informationen in der Wohnung.“⁶⁵ Ein Eingriff in diesen Schutzbereich ist somit jede hoheitliche Maßnahme, die den geschützten Bereich überwacht oder ausforscht.⁶⁶ Dieser Eingriff ist auch schon bei bloßer Anwendung technischer Mittel von außen gegeben⁶⁷. Eine Aushöhlung bzw. Umgehung des Grundrechtsschutzes darf nicht durch neue technische Möglichkeiten erreicht werden.⁶⁸ Denn im Grunde geht es auch bei der Online-Durchsuchung, auch wenn kein körperliches Betreten der Wohnung geschieht, „um die Ausforschung des Agierens bestimmter Personen, das sich nicht in der Öffentlichkeit abspielt, sondern in einem grundrechtlich besonders geschützten (Rückzugs-)Raum.“⁶⁹ Die Online-Durchsuchung als technisches Mittel beeinträchtigt somit den geschützten Bereich des Art. 13 GG⁷⁰.

Fraglich bleibt es aber, ob eine Online-Durchsuchung auf Computern, die in Geschäftsräumen stehen, ebenfalls das Grundrecht auf Unverletzlichkeit der Wohnung gem. Art. 13 GG beeinträchtigt. Es ist also grundsätzlich zu klären, ob der Schutzbereich des Art. 13 GG Geschäftsräume bzw. andere Räume als private, umfasst. Diese Frage ist insofern wichtig, als dass die Ermittlungsbehörden in den seltensten Fällen genau wissen

⁶² Eisenberg, Straf(verfahrens-) rechtliche Maßnahmen gegenüber „Organisiertem Verbrechen“, NJW 1993, 1033 (1038); Hermes, (Fn. 37), Art. 13. Rn. 57.

⁶³ Valerius, (Fn. 3), S. 275 (279).

⁶⁴ Valerius, (Fn. 3), S. 275 (280).

⁶⁵ Hermes, (Fn. 37), Art. 13 Rn. 33.

⁶⁶ Valerius, (Fn. 3), S. 275 (280).

⁶⁷ BVerfG, NJW 2004, S. 999 (1005f.)

⁶⁸ BVerfG, NJW 2004, S. 999 (1001).

⁶⁹ Kutscha, (Fn. 2), S. 1169 (1170).

⁷⁰ Valerius, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet, S. 127f.

wo sich der zu durchsuchende Computer befindet, und somit nicht klar ist welche Voraussetzungen vorliegen müssen, damit eine Online-Durchsuchung legitim wäre.

b. Geschäftsräume

Ob auch abgegrenzte Räume den Schutz des Art. 13 GG genießen, die nicht Wohnzwecken dienen, sondern auch oder ganz der „industriellen oder gewerblichen Produktion, des Handels oder der Dienstleistung, dem beruflich-wirtschaftlichen Bereich zuzuordnen und oft absichtlich dem Zutritt des Publikums geöffnet sind“⁷¹ ist umstritten. Das Bundesverfassungsgericht bejaht dies in ständiger Rechtsprechung⁷², wendet allerdings die Schranken der Art. 13 II und VII GG in einer gegenüber Wohnungen im engeren Sinne modifizierten Art und Weise an, weil das Schutzbedürfnis geringer sei.⁷³ Behördliche Besichtigungen und Prüfungen sollen nicht die Begriffe „Eingriffe und Beschränkungen“ des Art. 13 VII GG erfüllen, womit die Voraussetzungen von Art. 13 VII GG nicht vorliegen müssen. Vielmehr entnimmt das BVerfG dem Art. 2 I GG einen allg. Verhältnismäßigkeitsgrundsatz, der hier anzuwenden sein soll.

Die Gegenauffassung fasst nur die Wohnung im engeren Sinne unter Art. 13 GG.⁷⁴ Neben dem Wortlaut, sei die „Ausdehnung des Art. 13 GG auf Betriebsstätten und dem damit verbundenen Grundrechtsschutz für juristische Personen mit dem persönlichen Gehalt von Art. 13 GG nicht zu vereinbaren“⁷⁵.

„Dagegen spricht aber die in Art. 12 und 14 zum Ausdruck kommende Bedeutung, die Arbeit, Beruf und Gewerbe für die menschliche Selbstverwirklichung haben.“⁷⁶ Einzig auszunehmen sind aber die auf unkontrollierten öffentlichen Zutritt angelegten Betriebs- und Geschäftsräume, die zu der Zeit der Zugänglichkeit nicht den Schutz des Art. 13 GG genießen⁷⁷.

Es bleibt festzuhalten, dass gerade auch Computer in Betriebs- und Geschäftsräumen durch Art. 13 GG gedeckt sind. Zusätzlich zu der Ansicht, die die Betriebs- und Geschäftsräume in den Geltungsbereich des Art. 13 GG nimmt, ist selbst bei einer auf Publikumsverkehr ausgelegten Räumlichkeit davon auszugehen, dass der Inhaber keinen physischen Zugriff auf die sich dort befindlichen Computer duldet, und somit wiederum zur Verhinderung der Aushöhlung des Art. 13 GG auch ein virtueller Zugriff den Schutzbereich berührt.

⁷¹ *Hermes*, (Fn. 37), Art. 13 Rn. 23.

⁷² Exemplarisch: BVerfGE 32, 54 (69ff); 76, 83 (88).

⁷³ BVerfGE 32, 54 (75ff.).

⁷⁴ *Battis*, Schutz der Gewerberäume durch GG Art 13 und Wirtschafts-, Arbeits- und Steueraufsicht, *Jus* 1973, S. 25 (29f); *Hund*, Der Einsatz technischer Mittel in Wohnungen, *ZRP* 1995, S. 334 (336).

⁷⁵ *Hermes*, (Fn. 37), Art. 13 Rn. 26.

⁷⁶ *Pieroth/Schlink*, Grundrechte Staatsrecht II, Rn. 876.

⁷⁷ *Pieroth/Schlink*, (Fn. 75), Rn. 876.

2. Rechtfertigung von Beeinträchtigungen

„Die Verletzungshandlung besteht in einem [...] sich technischer Hilfsmittel bedienen unkörperlichen Eindringen in die Wohnung und dortiges Verbleiben durch die staatliche Gewalt. Sie wird durch die Speicherung und Verwendung der gewonnenen Informationen sowie durch deren Weitergabe an andere Stellen fortgesetzt.“⁷⁸ Obwohl die Online-Durchsuchung eher der allgemeinen Durchsuchung als den Lauschangriffen ähnelt, wird im Folgenden kurz auf die Voraussetzungen für einen Eingriff durch die so genannten Lauschangriffe einzugehen sein. Eine Anwendbarkeit dieser Rechtfertigungen auf die Online-Durchsuchungen ist fraglich, dennoch kann man diesen bisher bewährten Rechtfertigungen die generellen und evtl. zukünftigen Voraussetzungen für Online-Durchsuchungen entnehmen.

a. Besonders schwere Straftat, Art. 13 III GG

Nur wenn bestimmte Tatsachen den Verdacht begründen, dass der Verdächtige eine durch das Gesetz bestimmte besonders schwere Straftat begangen hat, und andere Möglichkeiten der Ermittlung nicht zu einem Ergebnis führen würden, darf eine Belauschung des Verdächtigen richterlich angeordnet werden.⁷⁹ Die technischen Mittel zur akustischen Überwachung müssten im Fall der Online-Durchsuchung angepasst werden. Allerdings erscheint es sinnvoll, eine solche Eingriffsschwelle auch für Online-Durchsuchungen anzulegen, da mit der Online-Durchsuchung ein nicht minder intensiver Eingriff in die Unverletzlichkeit der Wohnung des Verdächtigen gegeben ist.

b. Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, Art. 13 IV GG

Art. 13 IV GG dient der Wohnraumüberwachung zum Zwecke der Gefahrenabwehr.⁸⁰ „Der Einsatz technischer Mittel zur Überwachung von Wohnungen ist, wenn er präventiven Zwecken dient, nur unter den Voraussetzungen des Art. 13 IV GG zulässig.“⁸¹ Nach überwiegend vertretener Ansicht bezieht sich der Begriff der dringenden Gefahr i.S.d. Art 13 IV GG nicht auf einen bevorstehenden zeitlichen Eintritt, sondern auf die Intensität der drohenden Gefahr, also auf ihre Schwere.⁸² Als dringend ist eine Gefahr dann einzustufen, wenn eine erhebliche Gefahr mit hinreichender Wahrscheinlichkeit in allernächster Zukunft eintreten wird.⁸³

⁷⁸ *Pieroth/Schlink*, (Fn. 75), Rn. 877.

⁷⁹ *Gornig*, (Fn. 56), Art. 13 Rn. 94.

⁸⁰ *Hermes*, (Fn. 37), Art. 13 Rn. 75.

⁸¹ *Hermes*, (Fn. 37), Art. 13 Rn. 75.

⁸² *Gornig*, (Fn. 56), Art. 13 Rn. 124; BVerwGE 47, 31 (40).

⁸³ *Herdegen*, (Fn. 59), Art. 13 Rn. 77.

Aus präventiven Gründen erfolgt diese Überwachung nicht auf Grund von Anordnung durch drei Richter (Art. 13 III GG), sondern es reicht ein richterlicher Beschluss bzw. die sofortige Nachholung eines solchen. Alle Regelungen in Sicherheits- und Ordnungsgesetzen, die gegen diese Eingriffsschranke verstoßen, sind somit verfassungswidrig.⁸⁴

Im Bezug auf Online-Durchsuchung wird also festzuhalten sein, dass eine Überwachung, die als Ziel die Verhinderung dringender Gefahren für die öffentliche Sicherheit hat, auf Grund der Anordnung eines Richters stattfinden darf. Aus technischer Sicht wird allerdings vorerst fraglich bleiben, wie schnell der betroffene Computer lokalisiert werden kann bzw. ob der Verdächtige diesen bis zum „Gefahreintritt“ noch nutzt. Dies ist allerdings keine Frage der Verfassungsmäßigkeit sondern der Praktikabilität.

c. Unterrichtungspflicht des Bundes, Art. 13 VI GG

Kurz anzumerken bleibt, dass eine jährliche Unterrichtungspflicht der Bundesregierung an den Bundestag auch bei der Online-Durchsuchung als sinnvolle Maßnahme zur Kontrolle der Polizei- und Sicherheitsbehörden zu sehen ist.

3. Systemarten

a. Intern

Einige Stimmen der Literatur sehen einen unterschiedlichen Schutzbereich des Art. 13 GG in Bezug auf unterschiedliche Computersysteme. Zu unterscheiden sind grundsätzlich drei Systeme, das Interne, das Externe und das Mobile. Das interne System bildet hier den unproblematischen Fall, da es sich dabei um den Computer in den Wohnräumen des Betroffenen handelt, der auch nur dort benutzt wird. Daten werden lokal gespeichert, E-Mails werden abgerufen und ebenfalls lokal gespeichert, es werden keine externen Speichermedien benutzt. Wenn man die generelle Anwendbarkeit des Art. 13 GG auf Online-Durchsuchungen annimmt, was nach hiesiger Ansicht zu bejahen ist, dann wird das interne System unter den Schutzbereich des Art. 13 GG fallen.

b. Extern

Fraglich ist dies allerdings in Bezug auf das externe System. Unter dem Begriff „externes System“ versteht man, dass der Computer zwar physisch in der Wohnung des Betroffenen ist, bestimmte Daten aber teilweise online, auf Systemen Dritter abgespeichert werden. Einige Stimmen verneinen hierbei eine Anwendbarkeit des Art.

⁸⁴ Gornig, (Fn. 56), Art. 13 Rn. 131.

13 GG und verweisen auf das Hausrecht des Dritten.⁸⁵ Dabei ist allerdings zu unterscheiden. Sollte der Betroffene z.B. eine Homepage im Internet betreiben, die er auf Grund der Erreichbarkeit bewusst auf dem System eines Dritten ablegt, ist dieser Meinung wohl zu folgen.

Anders verhält es sich aber bei E-Mail Diensten. Anfänglich waren diese Dienste für den durchschnittlichen Benutzer noch relativ offensichtlich als extern gekennzeichnet, also auf dem System eines Dritten gespeichert, beispielhaft seien hier GMX, Yahoo oder Hotmail genannt. Allerdings entwickeln sich besagte E-Mail Postfächer mit teilweise direktem Zugriff (unter Umgehung der Anbieter Homepage) zu einer Ablage für persönliche Daten und E-Mails, wobei es dem durchschnittlichen Benutzer mittlerweile nicht mehr unbedingt klar sein muss, dass er den Schutzbereich seiner Wohnung, respektive seinen Computer, verlässt. Beispielhaft genannt sei hier der E-Mail Dienst „GMail“ des Anbieters Google. Denn besagte E-Mail Dienste buhlen mittlerweile mit der „direkten Einbindung“ in das Geschehen des Computernutzers, er muss also nicht mehr die Internet-Präsenz eines Anbieters aufrufen, dort seinen Benutzernamen und Passwort eingeben, sondern kann mit einem simplen Klick seine E-Mails von zu Hause direkt einsehen. Eine Benutzung eines lokal gespeicherten E-Mail Programms wäre nicht anders, und auch nicht mit mehr „Klick-Aufwand“ verbunden.

„Art. 13 wurde in das Grundgesetz eingefügt, um jedem Menschen ein letztes Refugium für die individuelle Entfaltung seiner Persönlichkeit im Kernbereich privater Lebensgestaltung zu verschaffen und zu sichern.“⁸⁶ Ein Zugriff von Polizei- und Sicherheitsbehörden auf diese Daten, und gerade der E-Mail Verkehr wird bei vermeintlichen Verdächtigen von besonderem Interesse sein, darf nicht damit gerechtfertigt werden, dass diese Daten nicht physisch in der Wohnung abgelegt sind, sondern muss sich am Empfinden des Betroffenen und Grundrechtsinhabers messen – und dieser wird die E-Mails als „in seiner Wohnung sicher verstaut“ sehen.

Die Argumentation, dass außerhalb der Wohnung aufbewahrte Briefe und Tagebücher auch nicht dem Schutzbereich des Art. 13 GG unterfallen⁸⁷, kann nicht überzeugen. Außerhalb der Wohnung aufbewahrte Briefe und Tagebücher unterliegen in keinem Fall solch einem direkten und ständigem Zugriff wie extern gespeicherte E-Mails. Der Vergleich ist allein auf Grund der heutigen technischen Möglichkeiten unzureichend.

Eine Online-Durchsuchung der E-Mails, die bei einem dritten Anbieter gespeichert sind (externe Systeme), wird sich nach hiesiger Meinung wohl am Grundrecht des Art. 13 GG zu messen haben.

⁸⁵ Rux, *Ausforschung* (Fn. 4), S. 285 (292).

⁸⁶ Rux, *Ausforschung* (Fn. 4), S. 285 (293).

⁸⁷ *Hornung*, *Erwiderung auf „Die Festplatte als Wohnung?“*, JZ 2007, S. 828 (829).

c. Mobil

Fraglich bleibt nun noch die Bewertung mobiler Systeme. Unter mobilen Systemen werden wohl z.B., Laptops, PDAs, Smartphones, Handys oder mobile Speichermedien wie USB-Sticks zu verstehen sein. Ein mobiles Gerät, das praktisch ständig innerhalb der Wohnung betrieben wird, ist wohl unproblematisch unter den Begriff des „internen Systems“ zu subsumieren. Dies ist aber anders zu beurteilen, wenn ein solches Gerät auch aus der Wohnung hinaus genommen wird. Eine Anwendung des Art. 13 GG, wie teilweise angenommen⁸⁸, scheint fragwürdig. Im Falle des mobilen Systems fehlt es an der ständigen Verfügbarkeit (s. externe Systeme). Vielmehr liegt eine Gleichbehandlung mit der externen Aufbewahrung von Gegenständen bei Dritten vor.⁸⁹ In diesen Fällen hat der Grundrechtsberechtigte willentlich die Daten aus dem Schutzbereich der Wohnung entfernt (an dieser Willentlichkeit fehlt es bei externen Systemen). Ein Zugriff im Rahmen einer Online-Durchsuchung auf mobile Systeme wird sich nicht am Grundrecht des Art. 13 GG zu messen haben.

Sollte der Fall vorliegen, der sogar relativ häufig sein dürfte, dass sich die Ermittlungsbehörden nicht sicher sind, welche Art von System vorliegt bzw. im Falle des mobilen Geräts, wo sich dieses gerade befindet, und somit nicht abzusehen ist, welches Grundrecht verletzt werden könnte, ist der Eingriff zu unterbleiben bzw. an den höchsten Schranken zu messen.

„Wenn nämlich eine staatliche Stelle bei Ihrem Handeln zwar nicht genau weiß, ob sie in ein bestimmtes Grundrecht – oder einfachgesetzlich begründetes Recht – eingreift, im konkreten Fall jedoch typischerweise damit rechnen muss [das ein bestimmtes Grundrecht verletzt werden könnte bzw. wird], so bleibt ihr nichts anderes übrig, als die insoweit bestehenden verfassungsrechtlichen oder einfachgesetzlichen Eingriffsvoraussetzungen einzuhalten.“⁹⁰

4. Kritik

Als Kritik gegen die generelle Anwendbarkeit des Art. 13 GG auf Online-Durchsuchungen wird vorgebracht, dass der Betroffene durch „Öffnung“ der Internet-Verbindung einen Zugriff erst ermöglicht hat, und seine Daten damit dem Internet zugänglich gemacht habe.⁹¹ Technisch bleibt zunächst zu sagen, dass mit der „Betretung“ des Internets die Daten des Computers keineswegs dem Zugriff preisgegeben sind, gerade

⁸⁸ Rux, Ausforschung (Fn. 4), S. 285 (293).

⁸⁹ Hornung, Erwiderung (Fn. 87), S. 828 (830).

⁹⁰ Hornung, Erwiderung (Fn. 87), S. 828, (830).

⁹¹ Hofmann, (Fn. 5), S. 121 (122/124); Lorentz im Rahmen einer Anhörung, NRW-LT-Drs. 14/3045.

um das zu verhindern bemühen sich Hersteller von Firewalls⁹², Virensclannern und Betriebssystemen. Allerdings ist der Zugriff dadurch möglich. Ein Computer der nicht mit dem Internet verbunden ist, kann ohne weiteres nicht durchsucht werden. In der Herstellung der Internetverbindung allerdings eine Art Fahrlässigkeit zu sehen, die das Durchsuchen erst ermöglichen, ist grundsätzlich falsch. „Zum Einen könnte dem Besitzer einer Wohnung andernfalls mit demselben Recht der Schutz des Art. 13 GG allein deshalb verwehrt werden, weil er diese Wohnung durch den Einbau von Fenstern und Türen nach außen geöffnet hat.“⁹³ Zum Anderen ist auch keine Einladung zur physischen Durchsuchung zu sehen, wenn der Wohnungsinhaber eines seiner Fenster auf „Kippe“ stellt, oder gar die Wohnungstür öffnet um diese zu verlassen. Diese Kritik an der Anwendbarkeit des Art. 13 GG ist somit abzulehnen.

Der Schutzbereich des Art. 13 GG findet auch in Bezug auf die Online-Durchsuchung Anwendung und muss im Rahmen der Gesetzgebung zur Schaffung von Ermächtigungsgrundlagen der Online-Durchsuchung Beachtung finden.

III. Informationelle Selbstbestimmung, Art. 2 I i.V.m. Art 1 I GG

1. Grundsatz und Herleitung

Das Recht auf „informationelle Selbstbestimmung“ wurde in der „Volkszählung, Mikrozensus“ Entscheidung des BVerfG am 15.12.1983⁹⁴ erstmal geprägt. Dort wird unter den Bedingungen moderner Datenverarbeitung der Schutz des Einzelnen bzgl. der unbegrenzten Erhebung, Speicherung und Verwendung sowie Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 I GG i.V.m. Art. 1 I GG hergeleitet. „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“⁹⁵

Um also eine Beeinträchtigung dieses faktisch bestehenden, aber nicht ausdrücklich normierten, Grundrechtes durch die Online-Durchsuchung zu rechtfertigen, bedarf es also gewisser Voraussetzungen. Eine Einschränkung des Rechts auf informationelle Selbstbestimmung sei nur im Rahmen des überwiegenden Allgemeininteresses zulässig.⁹⁶ „Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß (sic!). Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu

⁹² Eine Firewall ist eine Netzwerk-Sicherheitskomponente, die Netzwerkverkehr anhand eines definierten Regelwerks erlaubt oder verbietet, also gerade unbefugten Zugriff von außen verhindern soll.

⁹³ *Rux*, Ausforschung (Fn. 4), S. 285 (292).

⁹⁴ BVerfGE 65, 1.

⁹⁵ BVerfGE 65, Leitsatz 1.

⁹⁶ BVerfGE 65, Leitsatz 2.

beachten.“⁹⁷ Zu unterscheiden sei hier noch zwischen personenbezogenen individualisierten Daten und solchen, die für statistische Zwecke erhoben werden. Eine Online-Durchsuchung wird wohl grundsätzlich nur individualisierte Daten zu Tage bringen. Die Lockerung der Voraussetzungen für Daten, die zu statistischen Zwecken erhoben werden, ist also nicht einschlägig.

2. Anwendbarkeit

Die grundsätzliche Anwendbarkeit des Rechts auf informationelle Selbstbestimmung bzw. die Beeinträchtigung eben dieses ist bei der Online-Durchsuchung unproblematisch⁹⁸. Jede Online-Durchsuchung wird auch gleichzeitig das Recht auf informationelle Selbstbestimmung berühren – da das Ziel der Online-Durchsuchung eben die Feststellung von Daten ist.

3. Rechtfertigung von Beeinträchtigungen

Fraglich ist, wie eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 I i.V.m. Art. 1 I GG zu rechtfertigen ist. Von der Meinung, dass eine Online-Durchsuchung generell unzulässig ist, da sie einen Eingriff in die informationelle Selbstbestimmung darstellt, und nie zu rechtfertigen sei⁹⁹, ist Abstand zu nehmen.

Allerdings muss sich eine Online-Durchsuchung sehr wohl an diesem Grundrecht messen. Die Schranken für einen solchen Eingriff variieren nach der Art der Daten. „Je tiefer die Daten in den Persönlichkeitsbereich hineinreichen und je umfassender die Daten benutzt werden sollen [...], umso strengere Anforderungen stellt Art. 2 I an den mit der Datenerfassung usf. verfolgten Zweck und dessen gesetzliche Bestimmtheit.“¹⁰⁰ An den Zweck sind also umso höhere Anforderungen zu stellen, je tiefer die Daten gespeichert sind, und je intensiver sie benutzt werden sollen.¹⁰¹ Die Tiefe der Daten lässt sich wohl in drei Stufen gliedern¹⁰². Stufe eins umschreibt dabei die Adresse, einfache Merkmale wie Name, Vorname oder das Geburtsjahr. Stufe zwei beinhaltet beispielhaft Daten über „Krankheiten, Körperfunktionen und genetische Merkmale“¹⁰³ Die interessanteste und wohl auch häufigste Stufe ist die dritte, welche Daten aus dem „Mentalbereich über politische, weltanschauliche[...]“¹⁰⁴ beinhaltet.

⁹⁷ BVerfGE 65, Leitsatz 2.

⁹⁸ *Beulke, Meininghaus*, Verdeckte Durchsuchung eines Computers mittels heimlich installiertem Computerprogramm, StV 2007, S. 63 (64); *Schaar, Landwehr*, Anmerkung zum Beschluss des BGH vom 31.1.2007, K&R 2007, S. 202 (203); *Huber*, Trojaner mit Schlapphut – Heimliche Online-Durchsuchung nach dem Nordrhein-Westfälischen Verfassungsschutzgesetz, NVwZ 2007, S. 880 (882).

⁹⁹ *Bizer*, Gegen die Online-Durchsuchung, DuD 2007, S. 640.

¹⁰⁰ *Starck*, (Fn. 56), Art. 2 Rn. 116.

¹⁰¹ *Di Fabio*, in Maunz-Dürig GG-Kommentar, Art. 2 I Rn. 181.

¹⁰² *Starck*, (Fn. 56), Art. 2 Rn. 118.

¹⁰³ *Starck*, (Fn. 56), Art. 2 Rn. 118.

¹⁰⁴ *Starck*, (Fn. 56), Art. 2 Rn. 118.

Aus dem Gebot der Normenklarheit bzgl. einer Eingriffsermächtigung, als auch aus dem Verhältnismäßigkeitsprinzip ist zu entnehmen, dass das BVerfG einen legitimierte Zweck gesetzlich normiert sehen will.¹⁰⁵ Dies soll sicherstellen, dass die erhobenen Daten im Rahmen einer Online-Durchsuchung auch nur zu dem vorher festgelegten Zweck verwendet werden.¹⁰⁶

Eine mögliche Ermächtigungsgrundlage für Online-Durchsuchungen muss also, um dem Recht auf informationelle Selbstbestimmung zu genügen, festgelegte Zwecke normieren, auf Grund derer der Eingriff erfolgen soll. Des Weiteren ist zu entscheiden, ob für verschieden tiefe Eingriffe innerhalb der Ermächtigungsgrundlage verschiedene Voraussetzungen zu legen sind, oder ob generell von der höchsten Beeinträchtigung der Datentiefe ausgegangen wird. Letzteres erscheint nach der Ansicht des Verfassers vorzugswürdig, da der Übergang fließend sein dürfte. Die bloße Feststellung der persönlichen Daten wie Name, Vorname, Geburtsjahr o.Ä., wird nicht das Ziel einer Online-Durchsuchung sein. Das Ziel einer solchen Durchsuchung wird vielmehr die Aufklärung bzw. Verhinderung schwerer Straftaten sein, so dass grundsätzlich von der „dritten Datenstufe“, und somit von der höchsten Eingriffsstufe auszugehen ist.

D. Notwendigkeit neuer Ermächtigungsgrundlagen - Fazit

Die Notwendigkeit neuer Ermächtigungsgrundlagen für die Online-Durchsuchung ist besonders im Blickwinkel der jüngsten Entscheidung des BVerfG vom 31.01.2007 fast unumstritten. Eine Schaffung eben solcher kann auch nicht durch analoge Anwendung bereits vorhandener Ermächtigungsgrundlagen abgetan werden, sondern ist, wie vom BVerfG zutreffend festgestellt, eine Aufgabe der Legislative. Alleine schon aus dem Grund, dass die Gesetzgebung im Bereich der Online-Durchsuchung in Zukunft eine weit reichende Signalwirkung im Bezug auf das Verhältnis zwischen Staatsschutz und Unversehrtheit der Privatsphäre haben wird.

Aufgabe des Gesetzgebers ist es hier, einen Ausgleich zwischen dem Bedürfnis nach Schutz des Staats vor terroristischen Angriffen, und der Wahrung des privaten Lebensbereichs des Bürgers zu schaffen. Ziel kann es dabei nicht sein, vorschnelle Grundlagen für einen zu starken Eingriff zu schaffen. Der laute Ruf der Sicherheitsbehörden nach mehr Rechten und das evtl. momentan herrschende Gefühl der Unsicherheit beim Bürger in Fragen des Terrorismus dürfen keine Leit motive sein. Vielmehr ist an den bewährten Grundrechten festzuhalten und im Rahmen dieser für einige speziell normierte Fälle eine Online-Durchsuchung zu gestatten. Sie ist restriktiv

¹⁰⁵ *Di Fabio*, (Fn. 101), Art. 2 I Rn. 182.

¹⁰⁶ BVerfGE 65, 1 (46).

anzuwenden, und sollte nicht dazu gedacht sein, um z.B. den Steuerbehörden den sündigen Steuerzahler der Gemeinde X zu liefern. Denn das Gefühl, dass der Staat alles beobachtet, und auch alles beobachten darf, lässt das Gefühl der Freiheit, dessen Schutz eigentlich bewirkt werden soll, schwinden.

Die generelle Diskussion um die Online-Durchsuchung wird aber wohl auch mit der Schaffung einer Ermächtigungsgrundlage nicht schwinden – einen letzten Schlusstrich wird wohl erst das BVerfG setzen, nachdem die zukünftige Ermächtigungsgrundlage angegriffen worden ist.

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren

