Aug./Sept. 2007

Aufsätze und Entscheidungsanmerkungen

S. 329 Heft 8/2007

Die "Online-Durchsuchung". Verfassungsrechtliche Grenzen des verdeckten hoheitlichen Zugriffs auf Computersysteme

Von **Ulf Buermeyer**, Berlin*

Die "Online-Durchsuchung" scheint sich zu einem Dauerbrenner der innenpolitischen wie der rechtswissenschaftlichen Diskussion zu entwickeln: Zwar bestehen ganz erhebliche Zweifel, ob diese Ermittlungsmethode jemals effektiv wird angewendet werden können - zumal zur Bekämpfung der regelmäßig zur Legitimation ins Feld geführten sogenannten "Top-Gefährder" wie etwa Terroristen[1]. Dessen ungeachtet nehmen hinter Berliner Kulissen die Vorbereitungen für rechtliche Grundlagen sowohl für präventive als auch repressive Fernzugriffe auf Computersysteme Gestalt an. Neben den Unwägbarkeiten im tatsächlichen Bereich[2] treten dabei eine ganze Reihe von verfassungsrechtlichen Fragen auf, die eine gesetzliche Regelung der Online-Überwachung unter Geltung des Grundgesetzes in seiner derzeitigen Fassung nur in engen Grenzen realisierbar erscheinen lassen. An dieser Stelle soll auf die wichtigsten verfassungsrechtlichen Problemkreise hingewiesen werden.

1. Fernmeldegeheimnis, Art. 10 Abs. 1 GG

a) Schutzbereichsbestimmung durch das BVerfG

Brief-, Post- und Fernmeldegeheimnis gewährleisten nach der Rechtsprechung des Bundesverfassungsgerichts die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen und schützen damit zugleich die Würde des Menschen[3]. Hintergrund des Grundrechts ist die besondere Schutzbedürftigkeit der Vertraulichkeit der individuellen Kommunikation, wenn sie wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist. Denn damit unterliegt sie faktisch einem besonders leichten Zugriff Dritter[4]. Das Fernmeldegeheimnis des Art. 10 Abs. 1 GG schützt spezifisch die *unkörperliche* Fernkommunikation[5].

Der grundrechtliche Schutz knüpft dabei allein an die besondere Gefahr unkontrollierten Zugriffs durch unbefugte Dritte bei der Kommunikation über die Distanz an und ist in seiner Schutzrichtung für neue Entwicklungen und Gefährdungslagen offen[6]. Daher kommt es weder auf den übertragenen Inhalt noch auf das Medium oder seinen Betreiber an. Die Grundrechtsträger sollen sich vielmehr auf die Vertraulichkeit der Kommunikation über öffentliche Netze ebenso verlassen können wie auf diejenige über ihre privaten Netze[7]. Im Ergebnis sollen sie - in den Worten des Bundesverfassungsgerichts - "weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwesenden stünden"[8]. Geschützt ist allerdings nur das Vertrauen in die Sicherheit der Kommunikationsanlage, nicht hingegen das personengebundene Vertrauen in den Kommunikationspartner[9]. In diesem Rahmen umfasst der grundrechtliche Schutz sowohl den Inhalt als auch die näheren Umstände der Telekommunikation[10].

Nach der jüngsten Rechtsprechung des *Zweiten Senats des Bundesverfassungsgerichts* zur Beschlagnahme von Handyverbindungsdaten[11] endet der Schutz des Grundrechts jedoch in dem Moment, in dem die Nachricht beim Empfänger angekommen ist. Damit nämlich ende die besondere Schutzbedürftigkeit, die ihrerseits aus der spezifischen Gefährdung der Vertraulichkeit folgt, die sich aus dem erleichterten Zugriff Dritter bei Verwendung von Telekommunikationsmitteln ergibt. Einmal unangetastet

S. 330 Heft 8/2007

übertragene Daten, so der *Zweite Senat*, unterscheiden sich hinsichtlich ihrer Schutzbedürftigkeit nicht mehr von solchen, die der Nutzer selbst angelegt und niemals übertragen hat[12]. Einen Grenzfall stellt der Zugriff auf das zur Kommunikation verwendete Endgerät - etwa das Telefon - dar: Ob Art. 10 Abs. 1 GG hier Schutz bietet, ist - soweit stimmen beide Senate überein - mit Blick auf seinen Zweck und unter Berücksichtigung der spezifischen Gefährdungslage zu bestimmen[13]. Der *Zweite Senat des BVerfG* hat auf dieser Grundlage jedoch eine eher formale und tendenziell restriktive Differenzierung entwickelt: Werde der laufende Kommunikationsvorgang überwacht, so liege ein Eingriff in das Fernmeldegeheimnis auch dann vor, wenn die Erfassung des Nachrichteninhalts am Endgerät erfolgt. Sei die Nachrichtenübermittlung hingegen abgeschlossen,

so werde der Schutzbereich des Art. 10 Abs. 1 GG nicht mehr eröffnet[14].

b) Übertragbarkeit der Schutzbereichsabgrenzung auf den staatlichen Fernzugriff auf EDV-Anlagen

Bei der Frage, ob Fernzugriffe auf Rechner im Rahmen einer Online-Überwachung in den Schutzbereich der Telekommunikationsfreiheit fallen, ist nach den verschiedenen Formen des Zugriffs zu differenzieren.

aa) Fernzugriff auf gespeicherte Daten des Benutzers

Der *Zweite Senat* führt für die Unterscheidung zwischen Daten "unterwegs" und Daten "am Ziel" zwei Argumente an. Ihre Übertragbarkeit auf die tatsächlichen Gegebenheiten bei der Online-Überwachung kann aufschlussreich für die Frage sein, ob sich die darauf aufbauende rechtliche Differenzierung ebenfalls übertragen lässt.

aaa) Das Argument der Beherrschbarkeit

Zum einen stellt der *Senat* auf die Einflussmöglichkeiten des Betroffenen auf die gespeicherten Daten ab. Auf der Übertragungsstrecke sei die Herrschaft über die Daten in für das Fernmeldegeheimnis spezifischer und konstitutiver Weise eingeschränkt. Einmal übertragen sei jedoch ein unbemerkter Zugriff Dritter in der Regel nicht möglich. Außerdem könne der Betroffene die Daten jederzeit löschen und sie damit fremdem Zugriff entziehen. Er habe

"in seiner Herrschaftssphäre Möglichkeiten der Datenverarbeitung und -löschung - bis hin zur physischen Zerstörung des Datenträgers -, die ihm nicht zu Gebote stehen, solange sich die Nachricht auf dem Übertragungsweg befindet oder die Kommunikationsverbindungsdaten beim Nachrichtenmittler gespeichert sind. Der Nutzer kann sich bei den seiner Verfügungsmacht unterliegenden Geräten gegen den unerwünschten Zugriff Dritter durch vielfältige Maßnahmen schützen, etwa durch die Benutzung von Passwörtern oder anderweitiger Zugangscodes sowie - bei Verwendung von Personalcomputern - durch Einsatz von Verschlüsselungsprogrammen und spezieller Software zur Datenlöschung. **[15]** "

Es springt ins Auge, dass beides auf die Online-Überwachung gerade nicht zutrifft: Wie im technischen Teil des Beitrags im Einzelnen ausgeführt[16], verliert der Betroffene, dessen Festplatte mittels staatlichen Fernzugriffs überwacht wird, die Hoheit über seine Daten. Denn es ist gerade Sinn und Zweck der Online-Durchsuchung, die vom *Zweiten Senat* ins Feld geführte Beherrschbarkeit der Daten in der eigenen Sphäre des Betroffenen zu unterlaufen, um die so gewonnenen Daten kriminalistisch nutzbar zu machen. Der Betroffene kann daher seine Daten nicht mehr effektiv gegen den Zugriff Dritter schützen. Und er kann sie - einmal an die Sicherheitsbehörden übertragen - auch auf keine denkbare Weise mehr aus der Welt schaffen.

Dennoch verliert das Argument des *Senats* damit nicht seine Überzeugungskraft. Denn die erweiterten Möglichkeiten des Zugriffs, die die Beherrschbarkeit sowohl des Zugriffs als auch der Löschung durch den Berechtigten aushöhlen, knüpfen ihrerseits gerade nicht an Telekommunikationsvorgänge des Nutzers an. Sie sind - in der Terminologie der strafrechtlichen Zurechnungslehre - Formen alternativer Kausalität. Dass die Online-Durchsuchung die Unterschiede in der Beherrschbarkeit zwischen Daten "unterwegs" und Daten "daheim" nivelliert, hat nichts mit einer etwaigen telekommunikationsspezifischen Gefährdungslage dieser Daten zu tun, sondern allein damit, dass die Grenzen der persönlichen Herrschaftssphäre des Einzelnen durch die Online-Durchsuchung perforiert werden. Das aber ist keine Frage der Telekommunikationsfreiheit, sondern - wie noch zu zeigen sein wird - der Unverletzlichkeit der Wohnung.

bbb) Das Argument der Vergleichbarkeit mit niemals übertragenen Daten

Zum anderen bestünden für die bei den Teilnehmern gespeicherten Inhalte und Umstände der Kommunikation nicht mehr dieselben spezifischen Risiken, wie sie sich aus der Nutzung einer Fernmeldeeinrichtung als Kommunikationsmedium ergeben; vielmehr unterschieden sie sich nicht mehr von Dateien, "die der Nutzer selbst angelegt hat"[17].

Auch dieses Argument trifft unter den Bedingungen der Online-Überwachung weiter zu. In der Tat ist es für die Erfassung einer Datei durch einen Bundestrojaner gleichgültig, ob sie bereits einmal Gegenstand eines Telekommunikationsvorgangs war oder nicht. Damit aber ist die Gefährdungslage, der die beim Betroffenen gespeicherten Daten durch die Möglichkeit der Online-Überwachung ausgesetzt sind, jedenfalls nicht *spezifisch* für Telekommunikations(verkehrs)daten.

ccc) Fazit

Im Ergebnis trägt damit die Differenzierung des *Zweiten Senats des BVerfG* auch unter den Bedingungen der Online-Überwachung. Geht man - insofern in Übereinstimmung mit beiden Senaten des *BVerfG* ***[18]*** - davon aus, dass der Schutzbereich des Art. 10 Abs. 1 GG an eine für Telekommunikation spezifische Gefährdungslage anknüpft, so ist diese Voraussetzung für beim Betroffenen gespeicherte Daten - also die Zugriffsformen der *Spiegelung* und des *Monitoring* ***[19]*** - nicht erfüllt. Ihre Erfassung greift daher nicht in den Schutzbereich der Telekommunikationsfreiheit ein.

ddd) Die Ausleitung der erhobenen Daten als Eingriff in die Kommunikationsfreiheit?

Etwas anderes ergibt sich nicht etwa daraus, dass selbstverständlich sowohl für den staatlichen Zugriff auf das zu überwachende System als auch für die spätere Ausleitung der staatlicherseits erfassten Daten aus dem überwachten auf ein behördliches System wiederum Telekommunikation stattfindet. Denn es handelt sich in beiden Fällen gerade nicht um Kommunikation des Betroffenen, deren Verletzlichkeit zum Zugriff ausgenutzt würde, sondern um *hoheitliche* Datenübertragung, die in der nicht virtuellen Welt etwa der Anreise zum Ort des Zugriffs und dem späteren Abtransport beschlagnahmter Akten vergleichbar wäre. Schon von daher eröffnet allein der Modus des staatlichen Zugriffs nicht den Schutzbereich des Grundrechts aus Art. 10 Abs. 1 GG, macht er sich doch nicht die "spezifische Gefährdungslage"[20] zunutze, die für Daten "unterwegs" kennzeichnend ist. Anders formuliert: Allein aus der Tatsache, dass sich der Staat der Telekommunikation bedient, um Zugriffe auszuführen, folgt nicht, dass dieser Zugriff seinerseits einen Eingriff in Art. 10 Abs. 1 GG darstellte. Ein *Zugriff durch* Telekommunikation ist nicht notwendig auch ein *Eingriff in die Freiheit* der Telekommunikation.

eee) Zugriff "über Bande" auf Daten im Cyberspace

Ebenso wenig wird in den Schutzbereich eingegriffen, wenn Daten erfasst werden, die zwar nicht lokal gespeichert sind, auf die aber der Nutzer online zugreift. Zu denken wäre etwa an Daten auf einem entfernten Server, die lokal wie eine Festplatte eingebunden werden[21]. Zwar stehen diese Daten lokal nur zur Verfügung und können durch eine Online-Überwachung am Rechner des Betroffenen nur abgegriffen werden, indem sie ihrerseits per Datenfernübertragung in das überwachte System gelangen. Doch kann man sich bereits fragen, ob in dem Zugriff auf *eigene* ausgelagerte Daten des Überwachten - also gerade nicht auf einen Austausch zwischen zwei Kommunikationspartnern - überhaupt ein Eingriff im Sinne von Art. 10 Abs. 1 GG liegen kann. Versteht man den Begriff der Kommunikation aber so weit - wofür immerhin spricht, dass es für die Verletzlichkeit der Privatheit des Datenaustauschs keinen Unterschied macht, ob auf eigene ausgelagerte Inhalte des Beobachteten oder auf fremde Inhalte zugegriffen wird -, so macht sich aber doch die staatliche Überwachung hier nicht die spezifische Gefährdung der vom Nutzer initiierten Datenfernübertragung zunutze, sondern die erfolgreiche Infiltration des Zielsystems. Der Zugriff erfolgt zwar - bezogen auf die Kommunikation zwischen dem beobachteten Nutzer und dem ausgelagerten Speicher - am Endgerät. Doch könnten diese Daten auf dieselbe Weise erfasst werden, wenn sie dort lokal gespeichert wären, sodass gerade kein Eingriff unter Ausnutzung der für das Fernmeldegeheimnis konstitutiven Verletzlichkeit der Vertraulichkeit der Inhalte erfolgt.

bb) Überwachung der Internet-Telefonie

Anders hingegen liegt der Fall bei einer Überwachung der Internet-Telefonie auf dem System des Betroffenen. Inzwischen wird ein nennenswerter Anteil der Telefongespräche über das Netz so stark verschlüsselt, dass sie durch klassische Telekommunikationsüberwachung an der Infrastruktur des Netzes nicht mehr abgehört werden können. Daher besteht ein eindeutiges kriminalistisches Bedürfnis, diese Lauschlücke durch einen Zugriff auf die Endgeräte zu schließen: Nur hier werden die Inhalte wieder entschlüsselt und können durch geeignete Maßnahmen mitgeschnitten werden[22].

Auch eine Erfassung der Telekommunikation am Endgerät fällt jedoch nach der Rechtsprechung des BVerfG in den Schutzbereich des Art. 10 Abs. 1 GG[23]. Damit ist auch das Abhören von Internet-Telefonie durch Ausleiten der unverschlüsselten Inhalte aus einem der beteiligten Rechner als Eingriff in diesen Schutzbereich anzusehen. Denn ob an einem Telefon ein Abhörgerät[24] in *Hardware* - etwa als Miniatursender - oder in *Software* - etwa als Bundestrojaner - realisiert ist, macht aus grundrechtlicher Perspektive keinen Unterschied.

c) Rechtfertigung

Ein Eingriff in die Telekommunikationsfreiheit darf "nur auf Grund eines Gesetzes angeordnet werden", Art. 10 Abs. 2 Satz 1 GG. Beispielhaft bezogen auf die Telekommunikationsüberwachung zu repressiven Zwecken könnte eine solche Maßnahme vom Wortlaut der Eingriffs-

norm (§ 100a Abs. 1 StPO) - "Die Überwachung und Aufzeichnung der Telekommunikation darf angeordnet werden ..." - zwar noch gedeckt sein, da die Norm hinsichtlich der technischen Realisierung des Abhörens neutral formuliert ist. Andererseits macht § 100b StPO deutlich, dass die bisherige Ermächtigung zur Telekommunikationsüberwachung sich nur auf Eingriffe bezieht, die sich der Mitwirkung des Telekommunikationsdienstleisters bedienen. So muss nach Anordnung einer Telekommunikationsüberwachung "jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Überwachung und Aufzeichnung der Telekommunikation" ermöglichen (§ 100b Abs. 3 Satz 1 StPO). Außerdem muss die Anordnung neben Namen und Anschrift des Betroffenen "die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses enthalten" (§ 100b Abs. 2 Satz 1 StPO). Beides lässt sich jedenfalls nicht unmittelbar auf die

Internet-Telefonie anwenden. Zudem ist die exakte Identifizierung des zu überwachenden Rechners gerade eines der vielen ungelösten tatsächlichen Probleme der Online-Überwachung. In jedem Fall aber wäre sicherzustellen, dass tatsächlich ausschließlich in den Schutzbereich des Art. 10 Abs. 1 GG eingegriffen wird[25].

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

Eine zentrale Rolle in der Diskussion um die verfassungsrechtlichen Grenzen spielt die Unverletzlichkeit der Wohnung. Dies kann schon deswegen nicht verwundern, weil es sprachlich ("Durchsuchung") nahe liegt. Vor allem aber sprechen überzeugende Gründe für die Eröffnung des Schutzbereichs des Art. 13 Abs. 1 GG jedenfalls dann, wenn auf eine EDV-Anlage aus der Ferne zugegriffen wird, die sich innerhalb einer Wohnung im Sinne des Grundrechts[26] befindet.

a) Räumlicher Schutzbereich

In räumlicher Hinsucht erfasst der Schutzbereich des Art. 13 Abs. 1 GG Wohnungen. Nach der Rechtsprechung des BVerfG fallen unter diesen Begriff neben Wohnungen im natürlichen Sprachgebrauch auch Betriebs- und Geschäftsräume[27], nämlich insgesamt der Bereich der "räumlichen Privatsphäre"[28].

b) Schutzrichtung

Auch wenn historisch betrachtet Art. 13 Abs. 1 GG zunächst Schutz vor physischer Präsenz von Hoheitsträgern in einer geschützten räumlichen Sphäre bieten sollte, so hat das Bundesverfassungsgericht bereits 2004 in seiner Entscheidung zum "Großen Lauschangriff" betont, dass es für die Eröffnung des räumlichen Schutzbereichs des Grundrechts gleichgültig ist, ob in ihn durch körperliches Betreten oder unter Einsatz technischer Mitteln von innen oder von außen eingegriffen wird:

"Im Zeitpunkt der Schaffung des Grundgesetzes diente das Grundrecht des Art. 13 Abs. 1 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 Absatzes 1 umfasst wäre." **[29]**

Das Bundesverfassungsgericht hat damit den Schutzgehalt des Grundrechts im Lichte der fortschreitenden technischen Entwicklung offener ausgestaltet: Ging es traditionell um *Schutz gegen* das Betreten von Räumlichkeiten durch Hoheitsträger, also einen bestimmten Eingriffsmodus, so gewährt Art. 13 Abs. 1 GG nach der jüngeren Rechtsprechung auch explizit umfassenden *Schutz für* eine staatlichem Zugriff insgesamt entzogene räumliche Sphäre[30], ungeachtet der Frage, auf welche Weise ein Zugriff im konkreten Falle erfolgen mag.

Vor dem Hintergrund des Schutzzwecks des Grundrechts, das dem Einzelnen einen elementaren Lebensraum verbürgt und das Recht gewährleistet, in ihm in Ruhe gelassen zu werden[31], erscheint dies auch konsequent. Denn aus der Sicht des Betroffenen bedeutet der konkrete Modus des staatlichen Eindringens in diese oder des Erhebens von Informationen aus dieser Sphäre allenfalls einen graduellen Unterschied. Maßgeblich für die Beeinträchtigung der von Art. 13 Abs. 1 GG geschützten Vertraulichkeitserwartung ist die Beeinträchtigung der Privatheit und Intimität innerhalb der eigenen vier Wände. Nur weil die Erhebung bestimmter Daten aus dem geschützten Bereich einer Wohnung heraus aufgrund neuer technischer Möglichkeiten nicht mehr zwingend ein Betreten der Räumlichkeiten voraussetzt, führt dies gerade nicht dazu, dass solche neuen Eingriffsformen aus dem Schutzbereich des Grundrechts herausfallen: Einem solchen "Vorbehalt des technischen Fortschritts"[32] für die Unverletzlichkeit der Wohnung hat das BVerfG bereits mit der Entscheidung zum Großen Lauschangriff eine überzeugende Absage erteilt.

*c) Schutzbereichseröffnung bei Spiegelung und Monitoring **[33]** von Systemen innerhalb einer Wohnung*

Hält man sich dieses Verständnis des Schutzes der Unverletzlichkeit der Wohnung vor Augen, so greift ein

staatlicher Fernzugriff auf die gespeicherten Daten eines Rechners, der sich innerhalb einer Wohnung im Sinne des Art. 13 Abs. 1 GG befindet, zugleich in den Schutzbereich des Grundrechts ein[34].

aa) Eingriff durch Datenerhebung

Wie die Entscheidung zum Großen Lauschangriff treffend ausführt[35], macht es für die Verletzung der Privatheit innerhalb einer Wohnung gerade keinen Unterschied, auf welche Weise sie im einzelnen bewirkt wird. Damit kann es auch auf die Frage, ob auf die Daten einer EDV-Anlage innerhalb der geschützten Sphäre physisch - also durch Beschlagnahme und nachfolgende Auswertung - oder virtuell über Datenleitungen zugegriffen wird, letztlich nicht ankommen. Entscheidend für den Eingriff in den

von staatlichem Zugriff freien "elementaren Lebensraum"[36] ist vielmehr, dass sich die Daten innerhalb eines solchen Bereichs befinden und aus ihm heraus erhoben werden, sodass die Wohnung insoweit ihren Charakter als staatsfreien Rückzugsraum des Einzelnen verliert. Die Daten auf einem Rechner innerhalb einer Wohnung sind nicht etwa nur *partiell* gegen das Mitnehmen der Hardware im Rahmen einer Hausdurchsuchung geschützt, sondern umfassend gegen jede Form auch nicht physischen staatlichen Zugriffs.

bb) Schutzbereichsbegrenzung wegen verbleibender Rest-Privatsphäre?

Gegen diesen Eingriff in den Schutzbereich des Art. 13 Abs. 1 GG lässt sich nicht überzeugend einwenden, dass durch eine Online-Überwachung - im Gegensatz zum Großen Lauschangriff - nicht der gesamte räumliche Schutzbereich der Wohnung und damit auch nicht der gesamte Rückzugsbereich des Einzelnen negiert werde[37]. Zwar trifft selbstverständlich im Ansatz zu, dass die betroffene EDV-Anlage räumlich betrachtet nicht die gesamte Wohnung ausmacht, sodass in der Tat die von staatlichem Zugriff freie räumliche Sphäre nicht vollständig aufgehoben wird. Dennoch kann das Argument, es verbleibe ja noch ein anderweitiger Rückzugsraum, nicht dazu dienen, einem Eingriff in einen anderen Teil der Sphäre seine Eingriffsqualität abzusprechen. Dies zeigen folgende Überlegungen:

Zum einen kann der Einzelne angesichts der Heimlichkeit des staatlichen Zugriffs gerade nicht wissen, in welchem Umfang sein Rückzugsraum angesichts staatlicher Überwachung kein solcher mehr ist. Damit aber verliert er insgesamt seine Eigenschaft als Refugium, denn auch eine partielle Überwachung ließe sich naturgemäß nur umgehen, wenn man um ihren Umfang weiß.

Zum anderen macht eine Parallele zum Großen Lauschangriff deutlich, dass sich bei einem Zugriff auf einen räumlich umgrenzten Teil einer Wohnung allenfalls die Frage der Eingriffstiefe stellt, dies aber keinen qualitativen Unterschied ausmacht. So würde wohl niemand annehmen, eine Maßnahme falle nicht mehr unter Art. 13 Abs. 1 GG, wenn lediglich ein Teil einer Wohnung - etwa Küche und Wohnzimmer, nicht aber das Schlafzimmer - überwacht wird, da ja dann im Schlafzimmer eine von hoheitlichem Lauschen freie Zone verbleibe.

Entscheidend ist vielmehr, ob *überhaupt* Vorgänge innerhalb des räumlich geschützten Bereichs erfasst werden, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind[38]. So liegt es aber auch bei den auf einem Rechner innerhalb der Wohnung gespeicherten Daten. Denn auf "natürliche" Weise - also ohne staatlichen Zugriff in die räumlich geschützte Privatsphäre, ob *online* oder physisch - lassen sie sich nicht gewinnen.

Die Gegenansicht würde letztlich zu einer bedenklichen Verengung des Schutzbereichs des Art. 13 Abs. 1 GG führen, indem sie einen in einer Wohnung aufgestellten Rechner ohne Not als Exklave definiert, in der die im übrigen grundrechtlich gewährleistete Privatheit und Intimität nicht gewährleistet wäre. Zwar kann man - wie *Schlegel* treffend bemerkt - auch ohne Computer "allein sein"[39] - die Nutzung eines Computers ist für einen staatsfreien Rückzugsraum nicht konstitutiv. Dennoch wird ein Rechner, der in einer Wohnung genutzt wird, intuitiv und zu Recht als Teil der räumlichen Privatsphäre wahrgenommen, den die Wohnung im Übrigen bietet. Für die geschilderte Schutzbereichsbegrenzung fehlt es damit an jeder tatsachlichen Grundlage. Sie würde vielmehr dazu führen, empirisch gleiches verfassungsrechtlich ungleich zu behandeln.

cc) Die Online-Überwachung als Ersatzmaßnahme

Für diese Sichtweise sprechen weitere Gründe. So wären die Erkenntnisse, die durch eine online durchgeführte Untersuchung zu erlangen sind, ansonsten regelmäßig nur durch eine klassische Hausdurchsuchung zu gewinnen: Wären etwa die Daten statt auf dem infiltrierten Rechner in Papierform vorhanden, so könnten sie nur durch physische Sicherstellung gewonnen werden. Warum dieselben Daten einem geringeren Schutz unterliegen sollten, sobald sie auf einem Computer - und damit letztlich nur auf einem anderen Medium - innerhalb der geschützten Räumlichkeiten niedergelegt und damit technisch einfacher zu erlangen sind, lässt sich nicht überzeugend begründen. Die Online-Überwachung stellt eine typische Ersatzmaßnahme für eine Hausdurchsuchung dar[40]. Auch dies spricht für die Beibehaltung der grundgesetzlichen Anforderungen im Sinne einer gegenüber erweiterten technischen Zugriffsmöglichkeiten offenen Interpretation des Schutzbereichs des Art. 13 Abs. 1 GG, wie sie das BVerfG bereits seit der Entscheidung zum Großen Lauschangriff vertritt[41].

dd) Einwilligung in die Durchsuchung durch Anschluss an das Internet?

Kaum nachvollziehbar[42] erscheint demgegenüber das Argument, dass der Inhaber einer EDV-Anlage durch den Anschluss an das Internet in Kenntnis der Gefahren durch Viren und Trojaner eine Infizierung des Rechners "nolens volens in Kauf" nehme[43], also gleichsam auf den Schutz des Art. 13 Abs. 1 GG konkludent verzichte. Allein die technische *Möglichkeit* eines Zugriffs ist weder mit seiner rechtlichen *Zulässigkeit* gleichzusetzen noch gar mit der *Zustimmung* des Berechtigten. Um es zivilistisch zu formulieren: Kein objektiver Beobachter eines Internet-Nutzers würde ihm vernünftigerweise unterstellen, er habe damit konkludent seine Daten allgemeinem Zugriff über das Netz preisgeben wollen. Vielmehr hat der Gesetzgeber erst Anfang

August 2007 mit einer drastischen Verschärfung des Strafgesetzbuchs[44] nebst weitreichender Vorfeldkriminalisierung das Vertrauen der EDV-Anwender darin gestärkt, dass niemand sich unberechtigterweise Zugang zu EDV-Anlagen verschafft[45]. Für eine nicht staatliche "Online-Durchsuchung" droht seither Freiheitsstrafe von bis zu drei Jahren[46].

ee) Sonderfall mobile Rechner - Begrenzung des Schutzbereichs wegen Problemen der Standortbestimmung?

Nun können EDV-Systeme nicht nur ortsfest, sondern auch mobil und damit sowohl innerhalb als auch außerhalb des räumlichen Schutzbereichs von Art. 13 Abs. 1 GG betrieben werden - man denke nur an Laptops, aber auch an Mobilfunkgeräte mit Datenspeicher und PDAs. Es fragt sich daher, ob dies etwas an dem gefundenen Ergebnis ändert. So wird mitunter aus der Zufälligkeit des aktuellen Standorts eines mobilen Rechners der Schluss gezogen, damit sei die Unverletzlichkeit der Wohnung auf Computer *unabhängig* vom aktuellen Standort nicht anwendbar. Da es auf Zufälligkeiten nicht ankommen könne, schließe bereits die Möglichkeit des mobilen Einsatzes eine Schutzbereichseröffnung generell aus.

Überzeugen kann dies aus zwei Gründen nicht:

Zum einen ist schon die Prämisse irreführend, es handele sich bei dem Standort des Rechners um eine Zufälligkeit. Angesichts des räumlich definierten Schutzbereichs des Grundrechts aus Art. 13 Abs. 1 GG kommt dem Standort eines Rechners vielmehr aus gutem Grund eine zentrale Bedeutung bei. Wer seine Daten innerhalb der geschützten Sphäre verwahrt, darf grundsätzlich darauf vertrauen, von staatlichem Zugriff frei zu sein. Wer hingegen mit seinem Rechner diese Sphäre verlässt, gibt damit zugleich den besonderen Schutz auf, den diese Sphäre ihm bietet. Insofern ist es aus der Sicht des räumlich angelegten Schutzbereichs des Grundrechts gerade nicht zufällig, sondern allein sinnvoll, nach dem Standort der EDV-Anlage zu differenzieren[47].

Zum anderen lässt sich das unbestreitbare Dilemma für Hoheitsträger, den genauen Standort möglicherweise im Einzelfall nur schwer bestimmen zu können, auch in grundrechtsfreundlicher Weise auflösen. Es vermag nämlich nicht einzuleuchten, warum ein nach den tatsächlichen Umständen in den Schutzbereich des Art. 13 Abs. 1 fallender Rechner dennoch nicht als geschützt angesehen werden soll, nur weil andere Rechner - oder auch derselbe Rechner zu anderer Zeit - mobil betrieben werden. Andererseits spricht rechtlich nichts dagegen, im Zweifel die Anforderungen derjenigen tatsächlichen Konstellation zu erfüllen, mit deren Vorliegen mit einiger Wahrscheinlichkeit zu rechnen ist, auch wenn dies im Einzelfall objektiv nicht erforderlich sein sollte. Da nach wie vor ein signifikanter Anteil von EDV-Anlagen im räumlichen Schutzbereich des Art. 13 Abs. 1 GG betrieben wird, müssen daher die weitergehenden Voraussetzungen für einen Eingriff in dieses Grundrecht stets zugrundegelegt werden, sofern sich nicht im Einzelfall sicherstellen lässt, dass eine bestimmte Anlage nur außerhalb dieses Bereichs online überwacht wird[48].

d) Schutzbereichseröffnung bei Telekommunikationsüberwachung am Endgerät

Neben dem Zugriff auf die gespeicherten Daten steht das Abhören verschlüsselter Internet-Telefonie als sogenannte Telekommunikationsüberwachung an der Quelle - kurz "Quellen-TKÜ"[49] - im Zentrum des Interesses der Sicherheitsbehörden. Für eine eventuelle gesetzliche Grundlage ist daher zu fragen, ob sie neben Art. 10 Abs. 1 GG auch an der Unverletzlichkeit der Wohnung zu messen ist.

aa) Formale Betrachtung: Standort der Abhöreinrichtung

Für eine Eröffnung des Schutzbereichs könnte sprechen, dass auch eine Online-TKÜ sich jedenfalls technisch innerhalb der geschützten Sphäre einer Wohnung abspielt, wenn sich der zur Internet-Telefonie genutzte Rechner in einer Wohnung befindet.

bb) Schutzzweck der Unverletzlichkeit der Wohnung

Zu fragen ist jedoch, ob der Standort der zum Abhören genutzten technischen Einrichtung allein bereits den Schluss auf die Schutzbereichseröffnung zulässt. Denn in Bezug auf das Abhören von Wohnungen hat das Bundesverfassungsgericht entschieden, dass nicht auf die technische *Realisierung* der Überwachung abzustellen ist, sondern auf die so gewonnenen *Erkenntnisse*: Nicht der Standort des (Richt)Mikrofons gibt den Ausschlag für einen Eingriff in die Unverletzlichkeit der Wohnung, sondern die Tatsache, dass *"die Überwachung von außen solche innerhalb der Wohnung stattfindenden Vorgänge erfasst, die der natürlichen Wahrnehmung von außerhalb des geschützten Bereichs entzogen sind."*[50] Im Umkehrschluss bedeutet dies, dass allein die technische Realisierung einer Überwachung innerhalb einer Wohnung noch keinen Eingriff in die geschützte Sphäre bedeuten kann. Abzustellen ist vielmehr auf den Charakter der gewonnenen Erkenntnisse: Nur wenn sie in der Weise ein Teil der geschützten Sphäre sind, dass sich der Zugriff auf die Daten als Blick oder als Lauschen in die Wohnung darstellt, so fällt auch ihre Erhebung in den Schutzbereich des Art. 13 Abs. 1 GG.

Damit ist die eigentliche Frage, ob die Inhalte eines Telefongesprächs Teil der geschützten Sphäre der Wohnung sind. Dafür

ließe sich zwar wiederum anführen, dass sie in einer Wohnung gesprochen werden. Im Gegensatz zur nicht telefonischen Kommunikation innerhalb geschlossener Räume, bei der die Kommunikationspartner grundrechtlich geschütztes Vertrauen darin setzen, dass sie außerhalb des Raumes nicht mitgehört werden, werden Worte in ein Telefon aber gerade in der Erwartung und mit dem Ziel gesprochen, dass sie die geschützte Sphäre der Wohnung verlassen werden. Denn es ist ja gerade der Sinn der Telefonie, dass der *entfernte*, der *Tele*-Kommunikationspartner die gesprochenen Worte in der Ferne vernehmen kann. Wer über Telefonleitungen spricht - seien sie analog, digital oder virtuell im Netz -, vertraut daher auch nicht darauf, dass seine Worte die eigenen vier Wände nicht verlassen werden. Sein Vertrauen in die Vertraulichkeit seiner Worte gründet sich nicht auf die Schutz- und Abschlussfunktion der Wohnung. Er vertraut vielmehr auf die Zuverlässigkeit und Vertraulichkeit des Telekommunikationssystems. Dieses Vertrauen aber ist durch Art. 10 Abs. 1 GG geschützt und fällt nicht in den Schutzbereich der Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG. Damit ist das Abhören der Internet-Telefonie auch durch den Online-Zugriff auf das Endgerät allein an Art. 10 Abs. 1 GG und nicht an Art. 13 Abs. 1 GG zu messen.

cc) Kontrollüberlegungen auf der Wertungsebene

Das eben gefundene Ergebnis hält auch einer kritischen Betrachtung unter Wertungsgesichtspunkten stand: Es wäre in der Tat nicht nachvollziehbar, warum bestimmte Formen der Internet-Telefonie im Gegensatz zur klassischen Telefonie nicht abgehört werden können, allein weil dies aus technischer Sicht ein staatliches Tätigwerden innerhalb einer Wohnung erfordert, sofern dieses physische Eindringen in die Wohnung über die - als solche unstreitig nicht an Art. 13 Abs. 1 GG zu messende - bloße Erfassung der Telekommunikation hinaus keinen Einblick in die geschützte Sphäre gewährt.

Das so gefundene Ergebnis steht im übrigen auch im Einklang mit der bisherigen Rechtsprechung, wonach bei Gelegenheit einer zulässigen Telekommunikationsüberwachung akustisch wahrnehmbare Vorgänge innerhalb einer Wohnung nicht in den Schutzbereich des Art. 13 Abs. 1 GG fallen, also keinen "Großen Lauschangriff" darstellen.

Diese Überlegungen weisen den Blick zugleich auf die Schwierigkeiten der technischen Realisierung. Es wäre aus der Perspektive der soeben gefundenen Schutzbereichsbestimmung nämlich nicht etwa damit getan, das Mikrofon des betroffenen Rechners zu aktivieren, da es ja auch für Internet-Telefonie genutzt werde. Der Nutzer begibt sich vielmehr wie gezeigt des besonderen Schutzes der Unverletzlichkeit der Wohnung nur insoweit, als er tatsächlich und gegenwärtig per Internet-Telefonie kommuniziert. Es müsste also softwaretechnisch sichergestellt werden, dass lediglich diejenigen Vorgänge der Online-Überwachung der Telekommunikation unterliegen, die auch über die - als solche nicht abzuhörende - Internet-Strecke gehen.

e) Rechtfertigung

Die Frage der Schutzbereichseröffnung ist bei Art. 13 GG von besonderer Relevanz, weil eine Rechtfertigung eines Eingriffs nur unter engen Voraussetzungen möglich ist.

aa) Art. 13 Abs. 2 GG - "Durchsuchungen" von Wohnungen

Gem. Art. 13 Abs. 2 GG dürfen

"Durchsuchungen[...]nur durch den Richter, bei Gefahr im Verzuge auch durch die in den Gesetzen vorgesehenen anderen Organe angeordnet und nur in der dort vorgeschriebenen Form durchgeführt werden."

Eine "Online-Überwachung" könnte also nur dann auf der Grundlage von Art. 13 Abs. 2 gerechtfertigt werden, wenn sie auch als Durchsuchung im Sinne der Grundrechtsschranke anzusehen wäre.

Hiergegen spricht bereits der Wortlaut: Wie der *3. Strafsenat des Bundesgerichtshofs* in seiner Entscheidung zur strafprozessualen Zulässigkeit der "Online-Überwachung" anführt[51], liegt jedenfalls den §§ 102 ff. StPO die Vorstellung zugrunde, dass eine Durchsuchung offen und bei physischer Präsenz von Hoheitsträgern

durchgeführt wird[52]. Zwar müsste der Grundrechtsschranke nicht unbedingt dasselbe Begriffsverständnis zugrunde liegen wie der Strafprozessordnung. Doch bezeichnet der Begriff der "Durchsuchung" auch im Kontext des Art. 13 GG jedenfalls nur eine *offen* durchgeführte staatliche Erkenntnisgewinnung[53]. Es zeigt nämlich bereits das systematische Argument des Vergleichs mit Art. 13 Abs. 4 GG, der die "Überwachung" von Wohnungen unter weitaus engeren Voraussetzungen regelt, dass das Grundgesetz zumindest von einem Gegensatz zwischen der *offen* durchzuführenden "Durchsuchung" und der *heimlichen* "Überwachung" ausgeht.

Damit könnte eine Online-Überwachung allenfalls unter analoger Anwendung des Art. 13 Abs. 2 GG zu rechtfertigen sein. Das differenzierte Schrankensystem des Art. 13 GG lässt jedoch bereits das Vorliegen einer - zumal planwidrigen - Regelungslücke fernliegend erscheinen. Jedenfalls aber verbietet es die mit der Heimlichkeit der Online-Überwachung verbundene höhere Eingriffsintensität, von einer Vergleichbarkeit der Interessenlagen auszugehen. Gleiches gilt für die Tatsache, dass eine

klassische Durchsuchung einen punktuellen Eingriff in der Unverletzlichkeit der Wohnung darstellt, während eine Online-Überwachung jedenfalls dann von einiger Dauer ist, wenn sie über eine bloße Spiegelung hinausgeht.

bb) Art. 13 Abs. 3 GG - akustische Überwachung von Wohnungen

Die Schrankenregelung des Art. 13 Abs. 3 in der Fassung des "Großen Lauschangriffs" ermöglicht nur die "akustische" Wohnraumüberwachung. Eine online durchgeführte Spiegelung - von einem Monitoring oder noch weitergehender Überwachung ganz zu schweigen - ist daher vom Wortlaut nicht umfasst, allenfalls abgesehen von der Verwendung des eingebauten Mikrofons zur Überwachung der Umgebung.

Eine analoge Anwendung der Schranke zur Rechtfertigung einer Online-Überwachung dürfte wiederum an der Unvergleichbarkeit der Interessenlagen scheitern. Das Auslesen oder die noch weitergehende Überwachung eines Rechners ist im Vergleich zum Abhören einer Wohnung ein unvergleichlich andersartiger Eingriff: In mancher Hinsicht mag er zwar weniger eingriffsintensiv sein, weil weniger unmittelbare Lebensäußerungen zur Kenntnis von Hoheitsträgern gelangen. Dafür aber ergibt sich aus den auf einem Rechner gespeicherten Daten ein weitaus vollständigeres, differenzierteres und einen längeren Zeitraum abdeckendes Persönlichkeitsprofil, als es beim Abhören von Räumlichkeiten zu gewinnen ist.

cc) Art. 13 Abs. 4 GG - Überwachung von Wohnungen

Auf der Grundlage des Art. 13 Abs. 4 GG dürfen zur

"Abwehr dringender Gefahren für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr,[...]technische Mittel zur Überwachung von Wohnungen nur auf Grund richterlicher Anordnung eingesetzt werden."

Von vornherein würde dies die Zulässigkeit von Online-Überwachungen auf den präventiven Bereich begrenzen. Auch in diesem Rahmen müsste ein Fernzugriff auf einen innerhalb einer Wohnung befindlichen Computer als "Überwachung von Wohnungen" anzusehen sein.

Dies allerdings lässt sich kaum bestreiten: Sieht man einen innerhalb einer Wohnung verwendeten Rechner - wie hier vertreten - als Teil einer Wohnung an, sodass er Teil des räumlichen Schutzbereichs aus Art. 13 Abs. 1 GG ist, so lässt er sich konsequenterweise nicht von den Schranken ausnehmen, die dem Grundrecht selbst gesetzt sind: Lässt das Grundgesetz unter bestimmten Voraussetzungen einen Eingriff in eine Wohnung zu, so können an einen spezifischen hoheitlichen Zugriff auf einen Teil der Wohnung keine strengeren Anforderungen gestellt werden.

3. Schutz des Kernbereichs privater Lebensgestaltung

Eine ebenso hohe Hürde für eine "Online-Überwachung" *de lege ferenda* wird der auf der Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG beruhende sogenannte "Kernbereichsschutz" darstellen.

Aus der Menschenwürdegarantie folgt nach der Rechtsprechung des Bundesverfassungsgerichts zwar nicht, dass ein heimliches Vorgehen des Staates schlechthin unzulässig wäre, denn allein darin, dass der Mensch zum Objekt der Beobachtung wird, ist noch nicht zwingend eine Missachtung seines Wertes als Mensch zu erblicken[54]. Gleichwohl ist bei staatlichen Beobachtungen ein unantastbarer Kernbereich privater Lebensgestaltung zu wahren, denn würde der Staat in ihn eindringen, verletzte dies die jedem Menschen unantastbar gewährte Freiheit zur Entfaltung in den ihn betreffenden höchstpersönlichen Angelegenheiten. Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen[55]. Insbesondere ist kein Raum für eine Abwägung mit kollidierenden Rechtsgütern wie dem staatlichen Strafverfolgungsinteresse[56].

Ob ein Sachverhalt dem unantastbaren Kernbereich zuzuordnen ist, hängt davon ab, ob er nach seinem Inhalt höchstpersönlichen Charakters ist, also auch in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt[57]. In den Worten des Gerichts gehört zur

"Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung[...]die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen. Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität. **[58]** "

Demgemäß wäre beim staatlichen Fernzugriff sicherzustellen, dass dem Kernbereichsschutz unterfallende Informationen schon nicht erhoben werden. Für die erweiterten Zugriffsformen wie Aktivierung des Mikrofons oder der Webcam stellen sich damit vergleichbare Probleme wie beim "Großen Lauschangriff", es müsste also "live" überwacht und gegebenenfalls die Übertragung der Daten unterbrochen werden, denn der Eingriff in die Menschenwürdegarantie liegt gerade nicht erst in der Verwertung, sondern schon in der Erhebung entsprechender Daten: *"Nicht etwa darf in den absoluten Kernbereich privater Lebensgestaltung*

eingegriffen werden, um erst festzustellen, ob die Informationserhebung diesen Bereich betrifft."[59]

Ebenso wird man beim Einsatz eines *Sniffers/Keyloggers* die gesuchten Passwörter als solche zwar nicht der Intimsphäre zuordnen können, sodass deren Mitschneiden als solches keinen Bedenken im Hinblick auf den Kernbereichsschutz unterliegen wird. Um an die wenigen gesuchten Zeichen zu gelangen, müsste jedoch der gesamte "Tastaturverkehr" mitgelesen werden, also einschließlich etwaiger höchstpersönlicher Bekenntnisse in *Chatrooms* oder in *eMails*, die ihrerseits gerade nicht zur Kenntnis genommen werden dürfen - und zwar nicht einmal, um ihre Zugehörigkeit zum Kernbereich zu prüfen.

Soweit es um das Auswerten von gespeicherten Dateien geht, tut sich ein ähnliches Dilemma auf: Der Dateiname kann zwar grundsätzlich Aufschluss über den Inhalt geben. Zu denken wäre an eine Bezeichnung wie "TAGEBUCH.DOC". Andererseits hindert nichts einen Fundamentalisten daran, seine Bombenbauanleitung - vielleicht neben zahlreichen tatsächlich persönlichen Daten - unter gleichem Namen abzulegen. Sollen nun "intim" erscheinende Dateien generell von der staatlichen Kopie ausgenommen werden, was die Online-Überwachung erheblich weniger effektiv machen würde? Oder sollen alle potentiell relevanten Dateien doch übertragen und ausgewertet werden, was auf eine Verletzung des Kernbereichs hinausliefe, da ein Eingriff "probeweise" zwecks Prüfung der erhobenen Daten auf Zugehörigkeit zum Kernbereich gerade nicht zulässig ist?[60]

Schon diese Beispiele zeigen, dass der Kernbereichsschutz der Wirksamkeit staatlicher Fernzugriffe auf EDV-Anlagen enge Grenzen setzen dürfte. Denn wenn nicht sicher auszuschließen ist, dass eine Maßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst, so ist dieses Risiko verfassungsrechtlich allenfalls dann hinzunehmen, wenn ein Rechtsgut von besonders hohem Rang aufgrund konkreter Anhaltspunkte gefährdet erscheint. Dies müsste zudem ebenso formalgesetzlich geregelt sein wie die unverzügliche Löschung versehentlich erhobener kernbereichsrelevanter Inhalte[61].

4. Zusammenfassung

Der staatliche Fernzugriff auf EDV-Anlagen berührt je nach genauer Realisierung und Richtung des Zugriffs verschiedene grundrechtliche Schutzbereiche. Wird Internet-Telefonie mittels einer Software-Wanze - etwa eines Moduls eines "Bundes-Trojaners" - am Endgerät mitgeschnitten, ist nur der Schutzbereich der Telekommunikationsfreiheit eröffnet, sofern softwaretechnisch sichergestellt ist, dass auch lediglich solche Vorgänge erfasst werden können, die ihrerseits mit Wissen und Wollen des Nutzers Gegenstand der Telekommunikation sind. Alle anderen Zugriffe auf einen Rechner innerhalb einer Wohnung im Sinne des Art. 13 Abs. 1 GG eröffnen den Schutzbereich der Unverletzlichkeit der Wohnung. Sie sind daher von Verfassungs wegen nur unter den engen Voraussetzungen des Art. 13 Abs. 4 GG und insbesondere nur unter Wahrung des unantastbaren Kernbereichs der privaten Lebensführung zulässig. Letztere muss durch softwaretechnische Maßnahmen sicherstellen, dass keine zum Kernbereich zählenden Daten erhoben und versehentlich erhobene unverzüglich gelöscht werden.

---

* Der Verfasser ist Redakteur der HRRS und Richter in Berlin, wo er am Amtsgericht Tiergarten als Strafrichter tätig ist. An der Universität Leipzig arbeitete er von 1999 bis 2003 als Netzwerk-Administrator in einer gemischten Windows-Linux-Umgebung.

[1] Skeptisch zu bestimmten Formen der Online-Durchsuchung inzwischen auch der Bayerische Innenminister *Beckstein*, vgl. *Süddeutsche Zeitung* vom 1. September 2007, Seite 7.

[2] Vgl. zur tatsächlichen Seite der Online-Überwachung *Buermeyer* HRRS 2007, 154 m.w.N.; vgl. auch *Gercke* CR 2007, 245.

[3] BVerfGE 115, 166, 182.

[4] BVerfGE a.a.O.

[5] BVerfGE 115, 166, 182 f., von *Mangoldt/Klein-Gusy* 5. Aufl. Art. 10 Rn. 39.

[6] BVerfGE 115, 166, 182 f.

[7] *Gusy* (Fn. 5) Rn. 41.

[8] BVerfGE 115, 166, 182.

[9] BVerfGE 16, 28, 38.

[10] BVerfGE 115, 166, 183.

[11] BVerfGE 115, 166 ff.

[12] BVerfGE 115, 166, 184 f.

[13] BVerfGE 106, 28, 38 (Erster Senat); BVerfGE 115, 166, 187 (Zweiter Senat).

[14] BVerfGE 115, 166, 186 f.

[15] BVerfGE 115, 166, 185.

[16] *Buermeyer* HRRS 2007, 154, 161.

[17] BVerfGE 115, 166, 185.

[18] Oben Fn. 13.

[19] Zur Terminologie vgl. *Buermeyer* HRRS 2007, 154, 160 ff. In der Exekutive des Bundes werden die Begriffe "Online-Durchsicht" und "Online-Überwachung" verwendet., vgl. hierzu etwa http://netzpolitik.org/wp-upload/fragen-onlinedurchsuchung-BMJ.pdf.

[20] BVerfGE 115, 166, 187.

[21] Sogenanntes *"Mounten"*: Einem Datenspeicher im Netzwerk wird z.B. unter *Windows* mittels Menü oder des Befehls *"net use"* ein Laufwerksbuchstabe oder unter *Linux* mittels *smbmount* ein lokales Verzeichnis (Mount-Punkt) zugewiesen. Dann ist allenfalls noch an der geringeren Zugriffsgeschwindigkeit zu erkennen, dass nicht mit lokalen, sondern entfernten Daten gearbeitet wird.

[22] Zum technischen Hintergrund vgl. *Buermeyer* HRRS 2007, 154, 160 f.

[23] BVerfGE 106, 28, 37 (Erster Senat); 115, 166, 187 (Zweiter Senat).

[24] So ausdrücklich der Erste Senat des BVerfG in BVerfGE 106, 28, 38.

[25] Vgl. hierzu unten 2. d, vor allem Unterpunkt cc).

[26] Im folgenden wird der Begriff der Wohnung stets in diesem Sinne verwandt, ohne dies durch Anführungszeichen zu kennzeichnen.

[27] BVerfGE 32, 54, 69 ff.; BK-*Herdegen* 71. Lfg. Art. 13 Rn. 34; *von Mangoldt/Klein-Gornig* 5. Aufl. Art. 13 Rn 22 und 26.

[28] BVerfGE 32, 54, 72; BK-*Herdegen* 71. Lfg. Art. 13 Rn. 26.

[29] BVerfGE 109, 279, 309.

[30] *Gornig* (oben Fn. 27) Rn. 1.

[31] BVerfGE 109, 279, 309.

[32] So treffend *Schantz* KritV 2007, 343, 351.

[33] Zur Terminologie vgl. *Buermeyer* (oben Fn.19).

[34] Ebenso *Bär* MMR 2007, 239, 240; *Hornung* DuD 2007, 575, 578; *Jahn/Kudlich* JR 2007, 57, 60; *Rux* JZ 2007, 285, 292; *Schantz* KritV 2007, 343, 347 f; a.A. *Schlegel* GA 2007, Heft 11 (im Erscheinen).

[35] Vgl. oben Fn. 29.

[36] So die Terminologie des BVerfG, vgl. BVerfGE 109, 279, 309.

[37] So aber *Schlegel* GA 2007, Heft 11 unter D II. (im Erscheinen).

[38] BVerfGE 109, 279, 327; *Schantz* KritV 2007, 343, 347.

[39] GA 2007 Heft 11 unter D II 4. am Ende, (im Erscheinen).

[40] Ebenso *Schantz* KritV 2007, 343, 348.

[41] Vgl. oben bei Fn. 29.

[42] Ebenfalls kritisch *Hornung* DuD 2007, 575, 578; *Rux* JZ 2007, 285, 292; Schantz KritV 2007, 343, 349; noch deutlicher *Schlegel* GA 2007 Heft 11 (im Erscheinen) unter D I.: "Absurdität".

[43] So aber Hofmann NStZ 2005, 121, 124.

[44] 41. Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität vom 7. August 2007, BGBl. I 1786, in Kraft seit dem 11. August 2007.

[45] §§ 202a bis 202c sowie 303a StGB n.F.

[46] § 202a Abs. 1 StGB

[47] Ähnlich *Hornung* JZ 2007, im Erscheinen, in seiner Replik auf *Rux* (Fn. 11).

[48] Wie hier *Hornung* DuD 2007, 575, 578.

[49] So die Bezeichnung des Bundesministeriums des Innern in der (auf Vorarbeiten des Bundeskriminalamts zurückgehenden) Antwort auf Fragenkataloge des Bundesministeriums der Justiz und der Fraktion der SPD im Deutschen Bundestag, vgl. oben Fn. 19.

[50] BVerfGE 109, 279, 327.

[51] BGH StB 18/06 - Beschluss vom 31. Januar 2007, HRRS 2007 Nr. 197.

[52] A.a.O. Rn. 5.

[53] BK-*Herdegen* 71. Lfg. Art. 13 GG Rn. 52.

[54] BVerfGE 109, 279, 313.

[55] BVerfGE 109, 279, 313.

[56] BVerfGE 109, 279, 314.
[57] BVerfGE 109, 279, 313; 113, 348, 391.
[58] BVerfGE 109, 279, 313 f.
[59] BVerfGE 109, 279, 323.
[60] BVerfGE 109, 279, 323.
[61] BVerfGE 113, 348, 392.

[<<] 1 2 3 4 5 6 7 8 9 10 [>>]