Oktober 2009

Aufsätze und Entscheidungsanmerkungen

S. 433 Heft 10/2009

Zur Rechtswidrigkeit der Quellen-Telekommunikationsüberwachung auf Grundlage des § 100a StPO

Von Richter **Ulf Buermeyer**, Berlin, und Prof. Dr. **Matthias Bäcker**, Mannheim *

A. Einleitung

Die Überwachung der Kommunikation im Internet sowie der Zugriff auf Computer über das Netz sind spätestens seit der Diskussion um die sogenannte Online-Durchsuchung[1] zum Dauerbrenner in der innenpolitischen Debatte geworden. Zur Klärung der verfassungsrechtlichen Fragen[2] hat das BVerfG mit seinem Urteil zum nordrhein-westfälischen Verfassungsschutzgesetz[3] (im Folgenden: Online-Durchsuchungs- bzw. OD-Entscheidung) einen maßgeblichen Beitrag geleistet. Auch wo die Entscheidung gewisse Spielräume lässt,

S. 434 Heft 10/2009

deutet sie vielfach an, in welche Richtung eine verfassungsgemäße Lösung gehen muss. Diese Aussagen werden in der Praxis jedoch nicht immer ernst genommen. Der Beitrag verfolgt das Ziel, die mitunter bedenklich selektive Rezeption der OD-Entscheidung am Beispiel eines amtsrichterlichen Beschlusses zu diskutieren, der die Frage nach der Zulässigkeit der sogenannten "Quellen-TKÜ" betrifft - gegenwärtig für die Praxis der Sicherheitsbehörden wohl der relevanteste Aspekt der OD-Entscheidung.[4]

I. Hintergrund: Praktisches Bedürfnis nach Telekommunikationsüberwachung an der Quelle

Der Begriff "Quellen-TKÜ" bezeichnet das Überwachen von Telefongesprächen, die nicht über klassische Telefonverbindungen (Festnetz bzw. Mobilfunk), sondern über das Internet geführt werden (sog. Voice-over-IP- oder kurz VoIP-Verbindungen). Bei VoIP ist es verbreitet, die Audio-Daten in den beteiligten Endgeräten[5] noch vor dem Versand der Daten über das Internet zu verschlüsseln. In einem solchen Fall ist das "klassische" Überwachen der Telekommunikation etwa beim Internet-Zugangsanbieter (§ 100a Abs. 1 i.V.m. § 100b Abs. 3 StPO) wenig effektiv: Zwar lässt sich dort der verschlüsselte Datenstrom mitschneiden und hieraus der VoIP-Datenstrom isolieren. Doch ist es nur mit erheblichem Aufwand oder - je nach eingesetztem Verschlüsselungsverfahren - gar nicht möglich, die Daten zu entschlüsseln und so die Sprache wieder hörbar zu machen.[6]

Die am weitesten verbreitete VoIP-Software ist derzeit das kostenlose Produkt *Skype*, das den Datenstrom gleichfalls verschlüsselt. Zwar ist inzwischen öffentlich geworden, dass das dort eingesetzte Verschlüsselungsverfahren offenbar eine "Hintertür" enthält, die es zumindest dem Anbieter der Software ermöglicht, Gesprächsinhalte zu rekonstruieren.[7] Bisher ist jedoch nicht bekannt geworden, dass deutsche Hoheitsträger diese Möglichkeit nutzen. Außerdem existieren alternative Verschlüsselungsverfahren, sei es als Erweiterungen der VoIP-Verfahren, sei es durch den Aufbau von sogenannten Virtuellen Privaten Netzwerken (VPN). Ein erfolgversprechender Zugriff auf verschlüsselt geführte Internet-Telefongespräche setzt daher zumindest aus praktischer Sicht den Zugriff auf eines der beteiligten Endgeräte voraus, um dort den noch bzw. bereits wieder entschlüsselten Telefonverkehr gleichsam "an der Quelle" abgreifen zu können und so die eingesetzte Verschlüsselung auf der Übertragungsstrecke leerlaufen zu lassen. Daraus leitet sich auch der hierfür gängige Begriff "Quellen-Telekommunikations-überwachung" oder kurz "Quellen-TKÜ" ab.

Angesichts ihres greifbaren praktischen Bedürfnisses haben die Sicherheitsbehörden in der Diskussion um die "Online-Durchsuchung" von Anfang an den Wunsch geäußert, mittels Quellen-TKÜ verschlüsselte Telefongespräche mitzuhören und zu diesem Zweck auch heimlich auf den Rechner eines des Gesprächspartner unmittelbar zuzugreifen. Zeitgleich zu dieser Diskussion begannen offenbar noch während des laufenden Verfassungsbeschwerdeverfahrens zum nordrhein-westfälischen Verfassungsschutzgesetz die Arbeiten an der Umsetzung einer Quellen-TKÜ gegen die Telefonie-Software *Skype*: Im Januar 2008 veröffentlichte der *Chaos Computer Club* auf seiner Homepage ein Papier aus dem Bayerischen Staatsministerium der Justiz,[8] in dem die Kostenlast für die beim Einsatz eines "Trojaners" gegen *Skype* notwendige Hard- und Software (Polizei- oder Justizetat?) diskutiert wird. Die Authentizität des Dokuments einmal unterstellt, lässt sich aus der Sekundärfrage der Finanzierung folgern, dass seither "Trojaner" gegen *Skype* im Einsatz sind. Nach dem Papier belaufen sich die Kosten für eine

solche Maßnahme der Telekommunikationsüberwachung an der Quelle auf rund 6000 Euro monatlich; hinzu kommen rund 2500 Euro einmalige Kosten für die Installation der Überwachungssoftware sowie weitere unbezifferte Kosten für die Anmietung zweier Proxy-Server zur Verschleierung der Datenübertragung an das bayerische Landeskriminalamt.

II. Verfassungsrechtliche Problematik

In seinem Urteil vom 27. Februar 2008 geht das BVerfG nicht auf diese konkreten Umsetzungsbemühungen in Bayern, wohl aber auf die Frage der Zulässigkeit der Quellen-TKÜ überhaupt ein. Das Gericht widmet sich insbesondere der Abgrenzung zu noch weitergehenden Online-Zugriffen wie dem Mitschneiden von Tastatureingaben und dem Auslesen der Festplatte oder des Arbeitsspeichers. Es leitet aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) die neue Schutzdimension der Integrität und Vertraulichkeit des eigengenutzten informationstechnischen Systems - kurz:

das IT-Grundrecht - ab. In dieses "neue" Grundrecht greift die "Quellen-TKÜ" nur unter bestimmten engen Voraussetzungen *nicht* ein; hierzu werden besondere Sicherungen verlangt, die einen Eingriff ausschließen.[9]

Vor diesem Hintergrund schien die Debatte um die strafprozessuale Quellen-TKÜ *de lege lata* beendet - mangels spezifischer Ermächtigungsgrundlage sprach sich jedenfalls die Literatur einhellig für die Unzulässigkeit der Maßnahme auf der Grundlage des geltenden Rechts aus. Dann jedoch erschienen erste strafprozessuale Veröffentlichungen, die dieses scheinbar eindeutige Ergebnis in Frage stellten,[10] ohne sich mit der bis dahin einhelligen Literaturmeinung auseinanderzusetzen - und offenbar gestützt darauf ist kürzlich in Fachkreisen ein Beschluss eines Amtsgerichts bekannt geworden, das eine Quellen-TKÜ gegen *Skype* ausdrücklich für zulässig erklärt.[11]

Im Folgenden soll die amtsgerichtliche Entscheidung dokumentiert und analysiert werden, da sie aus zwei Gründen bemerkenswert erscheint: Zum einen ist nicht auszuschließen, dass ihr zumindest in dem betroffenen Bundesland Musterwirkung zukommen könnte, da sie offenbar auch in staatsanwaltschaftliche "Vorlagensammlungen" Eingang gefunden hat. Zum anderen zeigt die Entscheidung die Konsequenzen, wenn sich die strafprozessuale Diskussion bei der Rezeption eines verfassungsgerichtlichen Erkenntnisses von der verfassungsrechtlichen Literatur gleichsam lossagt: In Bezug auf die Quellen-TKÜ kann auf diese Weise ein Beobachter, der sich auf die spezifisch strafprozessuale Literatur beschränkt, den Eindruck gewinnen, es habe sich eine "herrschende Meinung" etabliert, die die Quellen-TKÜ auf der Grundlage des § 100a StPO für zulässig hält. Im Ergebnis tritt in der Bewertung der Quellen-TKÜ in der Literatur ein Schisma ein, gerade so, als gälte für strafprozessuale Eingriffe ein "Grundgesetz light".

B. Beschluss des Amtsgerichts

Die Entscheidung des Amtsgerichts wird hier nahezu im Wortlaut dokumentiert. Angesichts des laufenden Ermittlungsverfahrens haben die Verfasser alle Details entfernt, die einen Rückschluss auf das konkrete Verfahren zulassen könnten. Sie haben jedoch keinen Anlass zu zweifeln, dass im Anlassverfahren die Voraussetzungen einer "klassischen" Telekommunikationsüberwachung nach § 100a StPO vorliegen. Die Nummern in Klammern zu Beginn jedes Absatzes sind Hinzufügungen der Verfasser; orthografische Fehler wurden korrigiert.

Beschluss des Amtsgerichts vom 17. September 2009

In dem Ermittlungsverfahren gegen … wegen …

I. Der Beschluss des Amtsgerichts vom 28.05.2009 (Az Gs …) auf Überwachung und Aufzeichnung des Telekommunikationsverkehrs für die Rufnummer … des Anschlussinhabers …, verlängert durch Beschluss des gleichen Gerichts vom 19.08.2009 (Az. Gs …), wird wie folgt ergänzt:

Zur Überwachung der über den oben genannten DSL-Anschluss geführten verschlüsselten Telekommunikation wird die Vornahme hierzu erforderlicher Maßnahmen im Rahmen der Fernsteuerung angeordnet.

II. Zulässig sind jedoch nur solche Maßnahmen, die der Überwachung der Telekommunikation dienen und die für deren Umsetzung zwingend erforderlich sind. Unzulässig sind insbesondere die Durchsuchung des fremden Computers nach bestimmten gespeicherten Dateien sowie das Übertragen und Kopieren entsprechender Daten außerhalb eines Telekommunikationsvorgangs (Datenspiegelung und Datenmonitoring).

III. Zur Überwachung der über den oben genannten DSL-Anschluss geführten verschlüsselten Telekommunikation wird die Vornahme hierzu erforderlicher Maßnahmen im Rahmen der Fernsteuerung angeordnet.

Gründe:

(1) Die von der Staatsanwaltschaft beantragte Maßnahme ist zulässig. Das Amtsgericht - Ermittlungsgericht ist dabei nach § 162 Abs. 1 Satz 1 StPO zur Entscheidung berufen, da zwar eine Abhörmaßnahme am Computer des Beschuldigten innerhalb

seiner Wohnung stattfinden soll, damit jedoch ausschließlich die Telekommunikationsüberwachung beim Beschuldigten, nicht jedoch eine Überwachung des Wohnraums nach § 100c StPO i. V. mit § 74a Abs. 4 GVG erfolgen soll.

(2) 1. Die Anordnung der Maßnahme beruht auf § 100a StPO. Dessen Eingriffsvoraussetzungen in das Grundrecht nach Art. 10 GG umfassen auch die Internet-Telefonie und damit die sog. Quellen-Telekommunikationsüberwachung nebst den erforderlichen Begleitmaßnahmen (Meyer-Goßner § 100a Rn. 7 m.w.N.; Graf: in, Beck-Onlinekommentar § 100a Rn. 31, 114; Nack, in: Karlsruher Kommentar § 100a Rn. 27; Bär, in KMR § 100a Rn. 30).

(3) Der Beschuldigte ist aufgrund bestimmter Tatsachen verdächtig, Täter einer Katalogstraftat gem. § 100a Abs. 1[…]StPO zu sein, nämlich[…].

(4) Der Tatverdacht beruht auf dem Ergebnis der bisherigen Telekommunikationsüberwachung sowie der Mitteilung eines der [Kriminalpolizei]namentlich bekannten Zeugen, dem hinsichtlich seiner Personalien Vertraulichkeit zugesichert worden ist. Die bisherigen Ermittlungen haben ergeben, dass der Beschuldigte als Adressat der Maßnahme sich bei der Kommunikation der Sprachübertragung in Echtzeit mittels IP-Protokolls (VoIP) bedient, einer Form der Sprachübertragung über das Internet, wobei die eingesetzte Software (Skype) die Daten verschlüsselt (Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren Rn. 121 ff.; Nack, in: Karlsruher Kommentar zur StPO § 100a Rn. 16).

---

(5) Die Tat wiegt auch im vorliegenden Fall schwer, weil[…].

(6) Auf Grund der dargestellten bisherigen Ermittlungen ergeben sich auch keine tatsächlichen Anhaltspunkte dafür, dass durch diese Anordnung der Überwachung allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung gewonnen werden (§ 100a Abs. 4 Satz 1 StPO), weil die Maßnahme auf die im Tenor angegebenen Umfang beschränkt wurde und der Beschuldigte offensichtlich auf diesem Wege auch seine[Straftaten]mitorganisiert.

(7) 2. Bei der vom Beschuldigten für die Kommunikation eingesetzten Software, mittels derer die Telekommunikation verschlüsselt wird, ist der Vorgang nach der Verschlüsselung für die Ermittlungsbehörden weder hör- noch lesbar. Für die technische Umsetzung der Überwachungsmaßnahme ist es daher zwingend erforderlich, die Aufzeichnung der Telekommunikation vorher vorzunehmen. Dazu besteht nur die Möglichkeit, mittels einer noch zu installierenden speziellen Software auf dem Rechner des Betroffenen die noch unverschlüsselten Daten an die Strafverfolgungsbehörden zu übermittelt. Die Installation dieser Software ist zulässig. Denn ohne die Installation des zusätzlichen Programms auf dem Rechner des Betroffenen kann die Überwachung der über das Internet geführten verschlüsselten Telefonate nicht erfolgen. Die Telekommunikationsüberwachung wäre mithin nicht möglich.

(8) Der Zulässigkeit steht auch nicht die Entscheidung des Bundesgerichtshofs vom 31.01.2007 (MMR 2007, S. 237 = HRRS 2007 Nr. 197) entgegen. Anders als dort geht es vorliegend nicht um eine zielgerichtete verdeckte Online-Durchsuchung eines Personalcomputers nach Beweismitteln, für die der BGH das Vorliegen einer gesetzlichen Befugnisnorm verneinte. Ziel der angeordneten Maßnahme ist allein die Überwachung der Kommunikation zwischen dem Beschuldigten und einem Dritten i. S. d. § 100 a StPO ähnlich wie bei einem Abhörgerät, das in ein Telefonendgerät eingebracht wird. Dass diese Maßnahme verdeckt erfolgt, steht dem nicht entgegen, denn Telekommunikations-Überwachungsmaßnahmen erfolgen schon ihrer Natur nach stets ohne Wissen der betroffenen Personen.

(10) 3. Einer speziellen gesetzlichen Regelung zur Installation der Software bedarf es nicht, denn der mit der Installation der entsprechenden Software verbundene ausschließliche Eingriff in das Fernmeldegeheimnis (Art. 10 GG) ist als Begleitmaßnahme zur Umsetzung der Überwachung gem. § 100a Abs. 1 StPO im Wege der Annexkompetenz zulässig, weil andere mildere Mittel nicht zur Verfügung stehen (vgl. BGHSt 46, 266[273 f.]für § 100c Abs. 1 Satz 1 Nr. 1b StPO a.F.). Dazu ist die Beschränkung der Maßnahme, wie im Tenor angeordnet, durch technische Maßnahmen sicherzustellen. Die Überwachung darf sich nur auf Daten eines laufenden Telekommunikationsvorgangs beschränken, es darf zu keinerlei Zugriff auf sonstige auf dem Rechner des Betroffenen gespeicherte Daten kommen, so dass keine Online-Durchsuchung vorgenommen wird (dazu BVerfG NJW 2008, 822, 826 = HRRS 2008 Nr. 160).

(11) 4. Der Anordnung steht auch nicht entgegen, dass der Gesprächsinhalt der verschlüsselten Telefonate nach der Installation des Programms ohne Beteiligung des Netzbetreibers an die Ermittlungsbehörden ausgeleitet wird. Zwar wird in der Kommentarliteratur überwiegend die Auffassung vertreten, § 100a StPO (a.F.) räume den Ermittlungsbehörden nicht die Befugnis ein, Telekommunikation ohne Zutun eines Netzbetreibers zu überwachen (Schäfer: in, Löwe/Rosenberg § 100a Rn. 9 und 31 f.; Meyer-Goßner § 100a Rn. 2; KK-Nack, 5.Aufl, § 100a Rn. 5; so auch Gercke CR 2007, 245, 252).

(12) Selbst wenn man dieser Auffassung folgt, ergibt sich hieraus aber nicht die Unzulässigkeit der angeordneten Maßnahmen. Denn vorliegend erfolgt die Überwachungsmaßnahme nicht unter Ausschluss des Netzbetreibers. Vielmehr wurde diesem bereits aufgegeben, die in seinem Herrschaftsbereich anfallenden Daten an die Ermittlungsbehörden auszuleiten. Der

entsprechende Anordnungsbeschluss dieses Gerichts wird vorliegend lediglich um eine zusätzliche Maßnahme erweitert. Die Daten des Netzbetreibers sind im entschlüsselten Zustand mit den Daten identisch, die mittels des auf dem Rechner des Betroffenen zu installierenden Programms ausgeleitet werden. Im Ergebnis dient die Maßnahme mithin nur der Entschlüsselung der auch beim Netzbetreiber anfallenden Daten (für die Zulässigkeit der Maßnahme auch Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, Rn. 318 m.w.N.).

(13) Die Anordnung war gem. § 33 Abs. 4 StPO ohne vorherige Anhörung des Beschuldigten zu treffen, um den Zweck der Untersuchungsmaßnahme nicht zu gefährden.

(14) Eine gerichtliche Entscheidung zu § 101 Abs. 4 Nr. 3, Abs. 5 StPO unterbleibt, da die Entscheidung über das vorläufige Unterlassen der Mitteilung der Maßnahme an die Berechtigten von der Strafverfolgungsbehörde selbst zu treffen ist.

C. Diskussion

Lässt man den Beschluss auf sich wirken, so entsteht zunächst der Eindruck einer"runden" Entscheidung, die die Kommentarliteratur auswertet und für sich betrachtet durchaus zu überzeugen scheint. Bei genauerer Analyse ergeben sich jedoch durchgreifende verfassungs- wie strafprozessrechtliche Bedenken.

I. Maßstab der OD-Entscheidung

Das Bundesverfassungsgericht hat in seiner Entscheidung zum nordrhein-westfälischen Verfassungsschutzgesetz versucht, eine Abgrenzung zwischen der "bloßen" Überwachung der Internet-Telefonie, die als solche allein an Art. 10 Abs. 1 GG zu messen ist, und weitergehenden Zugriffen auf das System der Zielperson zu treffen, die in den Schutzbereich des Grundrechts auf Integrität und Vertraulichkeit des eigengenutzten informationstechnischen Systems eingreifen. Dabei orientiert es sich an Schutzbereich und Schutzzweck des IT- Grundrechts, das als weitere Schutzdimension aus dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) abzuleiten ist.

1. Schutzgegenstand

Das IT-Grundrecht schützt in sachlicher Hinsicht jedes hinreichend komplexe informationstechnische System.[12] Damit ist der Schutzgegenstand bewusst entwicklungsoffen formuliert: Computer sind unproblematisch erfasst, ebenso aber auch andere elektronische Geräte, sofern ein Zugriff *"es ermöglicht, einen Einblick in wesentliche Teile der*

Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten".[13] Darunter fallen etwa auch Handys, solange sie nur nicht lediglich ein Telefonbuch enthalten: Ein typisches *Smartphone* mit Telefonbuch, Kalender, eMail-Speicher und einigen Gigabyte Speicherkapazität für Fotos und Filme etwa lässt ebenso weitgehende Schlüsse über die Persönlichkeit des Nutzers zu wie mancher Rechner.[14] Wesentlich ist dabei, dass eine so massive Datenerhebung nicht im konkreten Fall eintreten oder auch nur drohen muss; abzustellen ist vielmehr abstrakt auf die Leistungsfähigkeit des betroffenen Systems.[15]

2. Schutzrichtungen

Inhaltlich weist das IT-Grundrecht zwei unabhängige Schutzgehalte aus, denn es richtet sich gegen Verletzungen der *Integrität* ebenso wie der *Vertraulichkeit* des informationstechnischen Systems.

a) Integrität des Systems

Der Begriff der Integrität ist der Informationstechnik entlehnt und betrifft - in juristische Terminologie gewendet - die *Zurechenbarkeit* der auf dem betroffenen System gespeicherten Inhalte: Die Integrität des Systems ist bereits dann verletzt, wenn aufgrund der Infiltration nicht mehr zweifelsfrei zu klären ist, ob ein Berechtigter oder ein Dritter für einen gespeicherten Inhalt verantwortlich ist.[16] In den Worten des BVerfG wird die Integrität des geschützten informationstechnischen Systems angetastet *"indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen."* [17]

Die Schutzbereichsdimension "Integrität" schützt daher insbesondere vor dem Einbau von Hintertüren in informationstechnische Systeme und vor der Installation sogenannter "Trojaner".[18] Dies bereits deshalb, weil jede Überwachungssoftware in mehr oder weniger großem Umfang die Kontrolle des Zielsystems ermöglicht und zugleich *prinzipbedingt* Veränderungen am Zielsystem vornimmt oder voraussetzt, nämlich zumindest die notwendigen Manipulationen, um die Funktion des Trojaners selbst zu ermöglichen. Damit ist jedoch die Zurechenbarkeit der Speicherinhalte zum Kreis der berechtigten Nutzer des Systems aufgehoben - und zwar unabhängig von der Frage, ob tatsächlich auch Daten verändert wurden:[19] Derjenige, der einen nicht

autorisierten Zugangsweg kontrolliert, hat damit virtuell seinen Fuß in die Tür des Systems gesetzt.

b) Vertraulichkeit des Systems

Die Vertraulichkeit des eigengenutzten informationstechnischen Systems hingegen schützt *"das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben."*[20] Ein Eingriff liegt insoweit in Datenerhebungen aus einem informationstechnischen System, die nicht von einem Berechtigten autorisiert sind.[21]

3. Konsequenzen für die Zulässigkeit einer Quellen-TKÜ mittels eines "Trojaners"

Legt man die eben skizzierten Maßstäbe zugrunde, so berührt die Telekommunikationsüberwachung "an der Quelle" unter Einsatz eines Abhör-Trojaners *potentiell beide* Dimensionen des Schutzbereichs des IT-Grundrechts. Dazu führt das BVerfG wörtlich aus:

"Wird ein komplexes informationstechnisches System zum Zweck der Telekommunikationsüberwachung technisch infiltriert ("Quellen-Telekommunikationsüberwachung"), so ist mit der Infiltration die entscheidende Hürde genommen, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung geht weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere können auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen.

Nach Auskunft der in der mündlichen Verhandlung angehörten sachkundigen Auskunftspersonen kann es im Übrigen dazu kommen, dass im Anschluss an die Infiltration Daten ohne Bezug zur laufenden Telekommunikation erhoben werden, auch wenn dies nicht beabsichtigt ist. In der Folge besteht für den Betroffenen - anders als in der Regel bei der herkömmlichen netzbasierten Telekommunikationsüberwachung - stets das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden. Den dadurch bewirkten spezifischen Gefährdungen der Persönlichkeit kann durch Art. 10 Abs. 1 GG nicht oder nicht hinreichend begegnet werden." [22]

Andererseits ist nicht zu verkennen, dass auf der Wertungsebene kein Unterschied zwischen der Überwachung klassischer Telefoniedienste und der Internet-Telefonie besteht:[23] Naturgemäß genießen die kommunikativen Inhalte als solche auch von Verfassungs wegen keinen weitergehenden Schutz, nur weil die Gesprächspartner nicht telefonieren, sondern etwa "skypen". In diesem Spannungsfeld zwischen den erheblichen Gefahren der Ausweitung der Datenerhebung bei einer Quellen-TKÜ einerseits und dem Streben nach Gleichbehandlung aller TKÜ unabhängig von der Übertragungstechnik andererseits hat sich das BVerfG für eine verfahrensrechtliche Lösung entschieden: Zwar ist auch die Quellen-TKÜ letztlich *materiell* nur an Art. 10 Abs. 1 GG zu messen. Dies gilt jedoch nur dann, wenn es im Einzelfall gelingt,

den Eingriff in die Integritätsdimension des IT-Grundrechts, der in der Installation eines Trojaners stets angelegt ist, gleichsam "einzuhegen" und weitergehende Eingriffe in den Schutzbereich sicher zu verhindern. Solche weitergehenden Eingriffe könnten etwa in der Erhebung von Daten außerhalb eines laufenden Kommunikationsvorgangs (dann: Vertraulichkeitsdimension betroffen) oder in einer weitergehenden Beeinträchtigung der Systemfunktionen (Integritätsdimension) liegen. Daher ist die Beschränkung auf die "reine" Überwachung der Telekommunikation zwingend sowohl durch die technische Gestaltung des Verfahrens als auch durch gesetzliche Vorgaben sicherzustellen. In den Worten des Gerichts:

"Art. 10 Abs. 1 GG ist hingegen der alleinige grundrechtliche Maßstab für die Beurteilung einer Ermächtigung zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein." [24]

Man darf davon ausgehen, dass das Hilfsverb "muss" vom Ersten Senat an dieser zentralen Stelle nicht zufällig verwandt wird.

4. Positionen in der Literatur

Die verfassungsrechtliche Literatur vertrat nach dem Urteil des Ersten Senats einhellig die Auffassung, ohne Gesetzesänderung sei eine strafprozessuale Quellen-TKÜ unzulässig: Die Ermächtigungsnormen in §§ 100a, 100b StPO sind auf eine netzbasierte TKÜ zugeschnitten und enthalten daher keinerlei rechtliche Vorkehrungen, um die Integrität eines infiltrierten Endgeräts zu schonen und "Exzesse", also Datenänderungen oder Datenerfassungen über die bloße Überwachung der Telekommunikation hinaus, auszuschließen.[25] Daraus zogen - ohne Anspruch auf Vollständigkeit - zumindest *Th. Böckenförde*[26], *Hoffmann-Riem*,[27] *Hornung*[28] und *Bäcker*[29] den Schluss, dass §§ 100a, 100b StPO den oben unter 3. skizzierten Anforderungen nicht genügen. *Sankol*[30] sowie das LG Hamburg[31] waren bereits vor der Entscheidung des BVerfG aus anderen Gründen im Ergebnis derselben Ansicht.

In der strafprozessualen Literatur hingegen bekamen die Reaktionen auf die OD-Entscheidung schnell eine andere Färbung:

Nack [32] stellte zwar ebenfalls fest, dass *"das BVerfG[für die Quellen-TKÜ]verlangt, dass die Einschränkung[auf Daten aus einem laufenden Kommunikationsvorgang]durch technische und rechtliche Vorgaben sichergestellt ist"*, und fand *"für die Zukunft eine gesetzliche Regelung angezeigt"- "für eine Übergangszeit"* allerdings meint er, auf die Erfüllung der grundgesetzlichen Vorgaben verzichten zu können,[33] gerade so, als handele es sich bei dem behördlichen Interesse an Maßnahmen der Quellen-TKÜ um einen Fall des Staatsnotstands.

Eine umfassende Aufzählung der Positionen im Schrifttum findet sich bei *Meyer-Goßner* in der Bearbeitung von *Cierniak* (56. Auflage), der die oben genannten Stimmen gegen die Tauglichkeit der geltenden StPO als Grundlage der Quellen-TKÜ sorgfältig zitiert, um sich dann jedoch - unter Verzicht auf die zeitliche Begrenzung *Nacks* - gleichwohl für die generelle Zulässigkeit der Quellen-TKÜ bereits nach geltendem Recht auszusprechen: § 100b Abs. 2 Satz 2 Nr. 3 StPO genüge den Vorgaben des BVerfG, denn er stelle sicher, *"dass sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt."*[34] Inwieweit allerdings die dort normierte Verpflichtung des Richters bzw. Staatsanwalts, in dem die TKÜ anordnenden Beschluss *"Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes"* anzugeben, wirklich geeignet ist, wirksam den Eingriff in die Integritätsdimension des IT-Grundrechts auf das unvermeidliche Maß zu begrenzen, erschließt sich nicht. Ebenso wenig leuchtet ein, inwieweit die zitierte Verfahrensregel Verletzungen der Vertraulichkeit des Systems verhindern könnte, damit tatsächlich nur in den Schutzbereich des Art. 10 Abs. 1 GG eingegriffen wird. Mit dem Verweis auf § 100b Abs. 2 Satz 2 Nr. 3 StPO wird der Schutz des IT-Grundrechts entgegen der Forderung des BVerfG maßgeblich dem Ermittlungsrichter überlassen, der über die Anordnung der Quellen-TKÜ entscheidet.

Weitgehend auf eine ernsthafte Auseinandersetzung mit der verfassungsrechtlichen Lage und den Differenzierungen des BVerfG verzichten schließlich *Graf*[35] und *Bär*.[36] Ersterer konstatiert optimistisch, aber im Gegensatz zu den vom BVerfG hierzu gehörten EDV-Sachverständigen:[37] *"Weitere Rechnerdaten werden durch eine[Quellen-TKÜ]nicht erhoben"*. Daher stehe *"der Quellen-TKÜ kein verfassungsrechtliches Hindernis entgegen"*. Zum Beleg beruft er sich auf die OD-Entscheidung, wenn auch mit erkennbarem innerem Vorbehalt ("so wohl auch BVerfG"). *Bär* zeichnet zwar die Vorgaben des BVerfG im Ansatz zutreffend nach, verzichtet aber (ohne dies explizit zu machen) auf dessen zentrale Anforderung, nämlich die *rechtliche* Regelung verfahrensrechtlicher Vorkehrungen zum Schutz der Integrität und Vertraulichkeit des Zielsystems. Es genüge vielmehr, wenn "dies durch die eingesetzte Software sichergestellt" werde.

II. Unzureichender Schutz des Zielsystems durch das Amtsgericht

Auch der Beschluss des AG entspricht den Vorgaben des BVerfG nicht. Die Anordnung beruft sich ohne nähere Diskussion auf die eben zitierten strafprozessrechtlichen Literaturstellen (vgl. Abs. 2) und entnimmt ihnen, dass sowohl die Überwachung der Telekommunikation mittels eines Trojaners als solche als auch die Installation der Trojaner-Software auf der Grundlage des §§ 100a, 100b StPO zulässig sei. Dass das Gegenteil der Fall ist, wurde eben bereits dargelegt.

Selbst wenn man mit dem AG §§ 100a, 100b StPO für eine taugliche Ermächtigungsgrundlage hielte, wäre zudem zu verlangen, dass die zentrale Anforderung des BVerfG nach Begrenzung der Infiltration des Systems auf die Quellen-TKÜ - und damit immerhin des Eingriffs auf einen solchen in Art. 10 Abs. 1 GG - wirksam umgesetzt wird. Denn mit der als solcher begrüßenswerten Tenorierung bestimmter Begrenzungen der Maßnahme (II. des Beschlusstenors) ist wenig gewonnen, wenn sich eine Quellen-TKÜ gar nicht durchführen lässt, ohne die Integrität und Vertraulichkeit des betreffenden Systems zu gefährden: Wenn Fremd-Software auf einem System installiert wird, so lässt sich nach Auskunft der in der mündlichen Verhandlung vor dem BVerfG gehörten Sachverständigen[38] *niemals* ausschließen, dass Daten des Systems erhoben oder verändert werden. Denn zumindest muss die Software selbst auf den Datenträgern gespeichert und im System so verankert werden, dass sie möglichst nicht auffällt, aber z.B. bei jedem Neustart des Systems wieder aktiviert wird, was bestimmte Kenntnisse über das System und Manipulationen seiner Einstellungen und Speicher voraussetzt. All diese Eingriffe stellen zugleich Veränderungen am System dar, die dessen Integrität verletzen. Nicht umsonst wird in der Literatur Skepsis geäußert, ob sich die Anforderungen der OD-Entscheidung an eine Quellen-TKÜ, die allein an Art. 10 Abs. 1 GG zu messen wäre, nach gegenwärtigem Stand der Technik überhaupt erfüllen lassen.[39] Es wäre Aufgabe des Ermittlungsrichters gewesen, sich zumindest davon zu überzeugen, welche konkreten Maßnahmen geplant sind und ob diese tatsächlich technisch sicherstellen, dass den Anforderungen des BVerfG genügt wird. Falls dies - was naheliegt - nicht möglich ist, bleibt ein einfacher Ausweg: Statt Unmögliches oder in sich Widersprüchliches auf die Gefahr hin anzuordnen, dass die gut gemeinten Begrenzungen in der Praxis missachtet werden müssen, ist der in Rede stehende Grundrechtseingriff abzulehnen.

Äußerst problematisch wäre schließlich, wenn bei einer Quellen-TKÜ - wie es das Papier des bayerischen Staatsministeriums der Justiz nahelegt - zu allem Überfluss Software von privaten Anbietern eingesetzt würde, die ohne den zugrundeliegenden

Quelltext geliefert wird und sich damit jeder eingehenden technischen Evaluation durch die Staatsanwaltschaft, die Polizei und das anordnende Gericht entzieht: Selbst bei bestem Willen könnte die Exekutive den Vorgaben eines Beschlusses wie des hier besprochenen oder auch - *de lege ferenda* - gesetzlichen Vorgaben dann nicht folgen. Sie wüsste selbst nicht, ob die eingesetzte Infiltrierungssoftware Kollateralschäden oder überschießende Datenerhebungen sicher vermeidet. Angesichts der grundrechtlichen Relevanz der notwendigen Eingriffsbegrenzungen verbietet es sich, hier auf wohlfeile Zusicherungen privater Vertragspartner zu vertrauen.

III. Installation eines Trojaners als "mitlegitimierter Voreingriff"

Kritisch zu betrachten ist weiterhin die in Abs. 10 näher ausgeführte Auffassung des AG, wonach die Installation der zur Quellen-TKÜ eingesetzten Software auf dem System des Betroffenen als "Sekundärmaßnahme" keiner *eigenständigen* gesetzlichen Ermächtigung bedürfe. Das AG bemüht hier einen Gedanken von *Bär,*[40] der die Installation eines Trojaners mit dem Einbau eines GPS-Positionssenders in einem Fahrzeug vergleicht und folgert, diese Umsetzungsmaßnahme sei von einer "Annexkompetenz" der Strafverfolgungsbehörden umfasst.

Dabei verkennt das Gericht jedoch, dass die Infiltration des Zielsystems einen eigenständigen Eingriff in das IT-Grundrecht in seiner Integritätsdimension bewirkt. Das IT-Grundrecht tritt nämlich gerade nur dann hinter Art. 10 GG zurück, wenn rechtlich sichergestellt ist, dass die Integrität und Vertraulichkeit des Zielsystems über die Quellen-TKÜ hinaus nicht beeinträchtigt werden.[41] Damit kommt man an dem Erfordernis einer eigenständigen Ermächtigungsgrundlage für die Quellen-TKÜ, die dann allerdings auch die Infiltration des Zielsystems decken würde, nicht vorbei.[42]

IV. Kernbereichsschutz

Die Ausführungen des Beschlusses zum Schutz des Kernbereichs privater Lebensgestaltung (Abs. 6) sind einfachrechtlich konsequent: Gemäß § 100a Abs. 4 Satz 1 StPO sind Maßnahmen unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass dadurch allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden. Dies ist hier nicht der Fall; im Gegenteil liegt die Erhebung kernbereichsrelevanter Inhalte bei einer Fallgestaltung wie der vorliegenden, wo soweit ersichtlich allein Gespräche zwischen Tatgenossen in Rede stehen, überhaupt fern.

Ungeachtet der einfachrechtlich wohl zutreffenden Anwendung des Gesetzes durch das AG ist jedoch insbesondere dem Gesetzgeber vorzuhalten, dass die "kernbereichsschützende" Regelung in § 100a Abs. 4 Satz 1 StPO ihrerseits nicht den verfassungsrechtlichen Anforderungen genügt. Ebenso wie andere neuere bundesrechtliche Normen[43]

---

lässt sie den Kernbereichsschutz auf der ersten Stufe[44] faktisch leerlaufen, denn wann werden bei einem Kontakt mittels Telekommunikation tatsächlich einmal *ausschließlich* kernbereichsrelevante Inhalte übermittelt? Auch Ehe- und Lebenspartner oder Gläubige und Seelsorger dürften sich vielmehr praktisch stets *zumindest auch* über Alltägliches wie das Wetter, das Abendessen oder den nächsten Einkauf unterhalten, was der Telekommunikationsüberwachung gemäß § 100a Abs. 4 StPO den Weg ebnet, mögen die übrigen Gesprächsinhalte auch intimster Natur sein.[45] Ein so offenkundig leerlaufendes, fast augenzwinkernd anmutendes Regelungsmodell enthält in der Sache eine kaum verhohlene Auflehnung des Bundesgesetzgebers gegen das BVerfG.[46]

V. Zugriff unter Umgehung des Providers

Strafprozessual nicht überzeugend erscheinen schließlich die Ausführungen des Beschlusses zur Frage, ob die Quellen-TKÜ in der angeordneten Form - also unter Einschaltung eines Trojaners - von den verfahrensrechtlichen Vorgaben des § 100b StPO gedeckt ist. Hier referiert das Amtsgericht zwar die einhellige Ansicht der Literatur, die Norm räume den Ermittlungsbehörden nicht die Befugnis ein, Telekommunikation ohne Zutun eines Netzbetreibers zu überwachen (Abs. 11). Bei der Subsumtion hierunter unterliegt es dann aber offenbar einem Missverständnis. Nach der zitierten Ansicht wäre die Quellen-TKÜ nämlich eindeutig abzulehnen gewesen, da bei dem gewählten Trojaner-Modell gerade *kein* Netzbetreiber mitwirkt: Die Installation erfolgt durch Hoheitsträger oder in ihrem Auftrag unmittelbar durch Dritte.[47] Die mitgeschnittenen Daten werden sogleich an die überwachende Behörde übermittelt - in der Praxis offenbar über mehrere Verschleierungs-Server als Zwischenstationen, wie man dem Papier des Bayerischen Staatsministeriums der Justiz entnehmen kann. Der Provider ist in diese Form der Quellen-TKÜ in keiner Weise eingebunden.[48]

Demgegenüber beruft sich das AG darauf, dass die Erhebung zwar nicht unter Einschaltung, aber auch nicht unter Ausschluss des Netzbetreibers vorgenommen werde, denn parallel zur Quellen-TKÜ werde auch eine klassische TKÜ durchgeführt, bei der dieselben Daten in verschlüsselter Form mitgeschnitten werden (Abs. 12). Letzteres mag zutreffen, doch kann das Argument gleichwohl nicht überzeugen: Dass parallel zu dem fraglichen Eingriff ein zweiter durchgeführt wird, gibt für die Zulässigkeit des ersten Eingriffs naturgemäß nichts her - insbesondere dann nicht, wenn es um die Vereinbarkeit der ersten Maßnahme mit einer

Verfahrensvorschrift geht und es sich verfahrenstechnisch um deutlich unterschiedliche Eingriffe handelt.

Aus demselben Grund kann auch das Argument des AG nicht überzeugen, dass es sich bei der Quellen-TKÜ letztlich um eine Entschlüsselung der beim Provider erhobenen Daten handele (Abs. 12): Wäre die unmittelbare Entschlüsselung dieser Daten möglich, bedürfte es gerade keiner Quellen-TKÜ. Gemeint ist offenbar, dass *materiell* dasselbe Ergebnis erzielt wird, wie es bei einer - fiktiven, da technisch nicht möglichen - Entschlüsselung zu erreichen wäre. Jedoch besagt auch die Zulässigkeit der staatlichen Kenntnisnahme von den Gesprächsinhalten auf einem Weg - nämlich der providergebundenen TKÜ - nichts über die in Rede stehende Kenntnisnahme auf einem anderen, gesetzlich gerade nicht ausdrücklich geregelten Weg, mag er auch im Ergebnis zu demselben Erkenntnisgewinn führen.

Ebenso unergiebig für die Vereinbarkeit der Quellen-TKÜ mit § 100b StPO ist schließlich die Tatsache, dass mit der (zulässigen) klassischen TKÜ die begehrten Daten gerade nicht erhoben werden können, sodass der Zugriff an der Quelle überhaupt erst notwendig wird. Dieser Gesichtspunkt mag rechtspolitisch dafür sprechen, eine Ermächtigungsgrundlage für die Quellen-TKÜ zu schaffen. Er hilft aber rechtlich nicht darüber hinweg, dass eine solche Ermächtigungsgrundlage bislang fehlt. Es ist nicht Sache des Ermittlungsrichters, selbst rechtsschöpfend tätig zu werden, um eine von ihm gesehene Ermittlungslücke zu füllen.[49]

D. Fazit

§ 100a StPO ist keine taugliche Grundlage für eine Quellen-TKÜ, sofern dazu Software auf dem betroffenen Endgerät installiert werden soll. So begreiflich der Wunsch der Sicherheitsbehörden sein mag, VoIP-Gespräche ebenso abhören zu können wie Festnetz- und Mobilfunktelefonate - im Rechtsstaat des Grundgesetzes trifft allein der Gesetzgeber die Entscheidung, in welche Grundrechte unter welchen Voraussetzungen eingegriffen werden darf. Sofern der politische Wille besteht, auch die Über-

wachung der Telefonie über das Internet zu repressiven Zwecken zuzulassen, müsste also der Bund eine spezifische Ermächtigungsgrundlage schaffen, die insbesondere den Vorgaben der OD-Entscheidung des BVerfG Rechnung zu tragen hätte. Jedenfalls ist es nicht Aufgabe des Richters, fehlende formalgesetzliche Ermächtigungsgrundlagen durch Beschlüsse zu ersetzen, in denen er den möglichen Gehalt einer geeigneten Befugnisnorm zu rekonstruieren versucht: Ermittlungseingriffe ohne gesetzliche Grundlage hat er abzulehnen.

* Der Autor *Buermeyer* ist Redakteur der HRRS, Richter des Landes Berlin und derzeit an die Senatsverwaltung für Justiz abgeordnet; der Beitrag gibt allein die persönliche Ansicht des Autors wieder. Der Autor *Bäcker* ist Juniorprofessor für Öffentliches Recht an der Universität Mannheim. Die zitierten URL waren am 20. Oktober 2009 gültig.

[1] Zu den Begrifflichkeiten und zum technischen Hintergrund vgl. eingehend *Buermeyer* HRRS 2007, 154 ff.

[2] Zum Diskussionsstand bis zur Entscheidung des BVerfG vgl. die Nachweise bei *Hornung* CR 2008, 299 bei Fn. 1.

[3] Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 = HRRS 2008 Nr. 160.

[4] Kürzlich wurde bekannt, dass das Bundeskriminalamt die seinerzeit im Fokus der Debatte stehende Online-Durchsuchung in Form des heimlichen hoheitlichen Zugriffs auf die Inhalte von Systemen bisher nicht ein einziges Mal durchgeführt hat, obwohl § 20k BKAG hierfür seit 1. Januar 2009 eine Ermächtigungsgrundlage enthält; vgl. http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/ein-streit-um-nichts.

[5] Dabei wird es sich gegenwärtig noch regelmäßig um Computer handeln. Allerdings bieten mehr und mehr leistungsfähige Mobilfunkgeräte wie etwa der N-Serie von *Nokia* oder auch das *iPhone* des Herstellers *Apple* Funktionen, um über den Internet-Zugang des Handys Internet-Telefondienste zu netzen. Der Mobilfunk-Provider O2 hat dies etwa vor kurzem offiziell als zulässige Nutzung seines mobilen Internet-Zugangs anerkannt.

[6] Zu technischen Einzelheiten vgl. bereits *Buermeyer* HRRS 2007, 154, 159 f. und *Sankol* CR 2008, 13.

[7] http://www.heise.de/security/meldung/Spekulationen-um-Backdoor-in-Skype-189880.html; vgl. hierzu auch *Hoffmann-Riem* JZ 2008, 1009, 1021.

[8] http://www.ccc.de/updates/2008/bayerntrojaner-wg-skype.

[9] BVerfG (Fn. 3), Rn. 188 ff; vgl. im Einzelnen unten S. 4 f.

[10] Vgl. im Einzelnen unter C. I. 4.

[11] *Bär* erwähnt entsprechende Beschlüsse des Ermittlungsrichters des BGH und des AG München bereits in der 52. Ergänzungslieferung des KMR (§ 100a StPO Rn. 32 a.E.), ohne Einzelheiten zu nennen.

[12] BVerfG (Fn. 3), Rn. 203; vgl. vertiefend *Bäcker* in *Uerpmann-Wittzack*, Das neue Computer-Grundrecht (2009), S. 1, 10 f.; *Hornung* CR 2008, 299 ff.

[13] BVerfG (Fn. 3), Rn. 203.

[14] BVerfG (Fn. 3), Rn. 203.

[15] BVerfG (Fn. 3), Rn. 203; *Hornung* CR 2008, 299, 302.

[16] *Bäcker* in *Uerpmann-Wittzack* (oben Fn. 12) S. 13 f.

[17] BVerfG (Fn. 3), Rn. 204.

[18] Zum Begriffsinhalt und zur Herkunft vgl. eingehend *Buermeyer* HRRS 2007, 154 ff.

[19] Ebenso *Böckenförde* JZ 2008, 925, 928.

[20] BVerfG (Fn. 3), Rn. 204.

[21] *Bäcker* in *Uerpmann-Wittzack* (Fn. 12), S. 13.

[22] BVerfG (Fn. 3), Rn. 188 f.

[23] *Buermeyer* RDV 2008, 8, 10; *Hoffmann-Riem* JZ 2008, 1009, 1021.

[24] BVerfG (Fn. 3), Rn. 190.

[25] Vgl. zu solchen Vorgaben hingegen § 20k Abs. 2 und 3 i.V.m. § 20l Abs. 2 Satz 2 BKAG und dazu *Bäcker,* Terrorismusabwehr durch das Bundeskriminalamt, 2009, S. 105 f.

[26] JZ 2008, 925, 934 bei Fn. 96, vgl. auch 937.

[27] JZ 2008, 1009, 1022.

[28] CR 2008, 299, 300 f.

[29] In *Rensen/Brink* (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts (2009), S. 99, 131 sowie in *Uerpmann-Wittzack* (oben Fn. 12), S. 22.

[30] CR 2008, 13, 17 f.

[31] MMR 2008, 423 m. abl. Anm. *Bär*.

[32] *Nack* in *Karlsruher Kommentar zur StPO*, § 100a StPO, Rn. 27.

[33] A.a.O (vorige Fußnote).

[34] *Meyer-Goßner*, Kommentar zur Strafprozessordnung, 56. Auflage, § 100a StPO Rn. 7.

[35] *Graf* in Beck'scher Online-Kommentar zur StPO, Edition 4 (Stand 15. Juni 2009), § 100a StPO Rn. 114.

[36] *Bär* in KMR, 52. Ergänzungslieferung (Dezember 2008), § 100a StPO Rn. 31.

[37] Vgl. BVerfG (Fn. 3), Rn. 189.

[38] Vgl. Rn. 189 und 240 der OD-Entscheidung.

[39] *Bäcker* in *Rensen/Brink* (oben Fn. 26) S. 131.; *Hoffmann-Riem* JZ 2008, 1009, 1022; *Hornung* CR 2008, 299, 300 f.

[40] Etwa in K/M/R (oben Fn. 36) Rn. 32; zur Terminologie vgl. auch *Sankol* CR 2008, 13, 14 ff.

[41] *Bäcker* in *Uerpmann-Wittzack* (oben Fn. 12) 21 f.

[42] Im Ergebnis wie hier AG Hamburg, Beschluss vom 28. August 2009 - 160 Gs 301/09 -, noch unveröffentlicht (erscheint in Heft 12/2009 des *Strafverteidigers*).

[43] § 20k Abs. 7, § 20 l Abs. 6 BKAG; § 23a Abs. 4a ZFdG.

[44] Zu dem zweistufigen Schutzkonzept vgl. BVerfGE 109, 279, 318 ff.; 113, 348, 390 ff.; BVerfG (Fn. 3) Rn. 270 ff.; *Bäcker* (oben Fn. 25) S. 80 ff.

[45] Vgl. zur Wohnraumüberwachung bereits BVerfGE 109, 279, 330.

[46] Kritisch etwa *Reiß* StV 2008, 539, 541 f.; *Wolter* GA 2007, 183, 196; ebenso zu § 20k Abs. 7 BKAG *Bäcker* (Fn. 25), S. 89; *Baum/Schantz* ZRP 2008, 137, 138; *Hoffmann-Riem* JZ 2008, 1009, 1021; *Piltz/Pfister* Recht und Politik 2009, 4, 5 f.; *Poscher* JZ 2009, 269, 276; *Roggan* NJW 2009, 257, 261.

[47] Vgl. zu den Infiltrationsmöglichkeiten eingehend *Buermeyer* HRRS 2007, 154 ff.

[48] Dabei soll nicht übersehen werden, dass die Manipulation des Datenstroms zum Nutzer unter Mitwirkung des Providers ein möglicher Weg ist, das System des Betroffenen zu infiltrieren, vgl. zum technischen Hintergrund *Buermeyer* HRRS 2007, 154, 163 f. unter c). Dies ändert jedoch nichts daran, dass die eigentliche Überwachung ohne jedes Zutun des Providers erfolgt. Außerdem verhält sich der Beschluss des AG nicht zu der Frage, wie der Trojaner für die Quellen-TKÜ auf das Zielsystem gelangt. Naheliegend wäre eher ein - ebenfalls von keiner Ermächtigungsgrundlage gedecktes - Betreten der Wohnung zum

"Verwanzen" des Rechners, was den Schutzbereich des Art. 13 Abs. 1 GG berühren würde.

[49] BGH 3 StR 552/08, Urteil vom 14. August 2009, HRRS 2009 Nr. 890 (in diesem Heft), Rn. 36 ff. Zwar nimmt der BGH hier - wie so oft - letztlich kein strafprozessuales Verwertungsverbot an, obwohl er selbst mangels verfassungsgemäßer Ermächtigungsgrundlage von einem rechtswidrigen Ermittlungseingriff ausgeht. Für die Frage, ob ein Eingriff überhaupt erst angeordnet werden darf, kann es ungeachtet der Folgefrage des Verwertungsverbotes aber nur auf die Rechtmäßigkeit des Eingriffs ankommen.

[<<] ... 3 4 5 6 7 8 9 10 11 12 13 ... [>>]