HUMBOLDT FORUM RECHT
- Die juristische Internet-Zeitschrift an der Humboldt-Universität zu Berlin -

HFR 19/2007 ISSN 1862-7617 Aufsatz

Professor Dr. Hans Kudlich, Erlangen

Zur Zulässigkeit strafprozessualer Online-Durchsuchungen

Die Online-Durchsuchung, als heimlicher staatlicher Zugriff auf informationstechnische Systeme über Kommunikationsnetze, wirft vielfältige Fragestellungen auf und wird in der rechtswissenschaftlichen Literatur kontrovers diskutiert. Dabei ist die rechtliche Balance zwischen Strafverfolgung und Grundrechtsschutz von besonderer Bedeutung. In dem vorliegenden Beitrag werden von Prof. Dr. Hans Kudlich ausgewählte Aspekte der Diskussion um Online-Durchsuchungen aufgegriffen und straf- sowie verfassungsrechtlich untersucht.

Der Autor beschäftigt sich zunächst mit verdeckten Online-Durchsuchungen de lege lata, zeichnet die Entscheidung des Ermittlungsrichters des BGH bzw. des 3. Strafsenates nach und würdigt diese kritisch. Es wird dargelegt, dass es sich dabei um keine Durchsuchung im Sinn der StPO handelt und eine analoge Anwendung der §§ 102, 105 I StPO, ein Rückgriff auf § 100a StPO und die strafprozessuale Ermittlungsgeneralklausel der §§ 161 I S. 1, 163 I StPO abgelehnt.

Prof. Dr. Hans Kudlich skizziert im Verlauf seines Beitrages wichtige Gesichtspunkte für eine eventuelle Einführung einer Befugnisnorm zur verdeckten Online-Durchsuchung de lege ferenda. Die notwendige Unterscheidung zwischen präventivem und strafprozessualem Bereich findet hierbei einführend Beachtung. Ob mit der Schaffung einer entsprechenden Befugnisnorm zugleich eine Verfassungsänderung einhergehen muss und hier insbesondere Art. 13 GG betroffen ist, wird in der Prüfung eines Eingriffs in den Schutzbereich von Art. 13 GG und der Besprechung der materiellen Verfassungsmässigkeit einer entsprechenden Regelung behandelt. Der Autor weist darauf hin, dass der vom Bundesverfassungsgericht geforderte Schutz des Kernbereichs der privaten Lebensgestaltung besondere Beachtung erfahren muss. Hinsichtlich der Anordnungskompetenz hebt er das Erfordernis eines Richtervorbehalts hervor, eine Eilzuständigkeit wird nicht zuerkannt.

I. Hinführung

1 Kaum eine strafprozessuale Entscheidung der jüngeren Vergangenheit hat in der strafrechtswissenschaftlichen Literatur[1] ein so breit gefächertes Echo und zugleich in der Tagespolitik so kontroverse Diskussionen[2] ausgelöst wie die vom 3. Strafsenat bestätigte Ablehnung einer beantragten „Online-Durchsuchung“ durch den Ermittlungsrichter am BGH vom 25. bzw. 28.11.2006. Der Grund für die regen und teilweise sehr engagierten Reaktionen mag vordergründig darin liegen, dass es sich zumindest um einen „besonders intensiv gefühlten“ Eingriff handelt[3], wenn dem Beschuldigten von den Strafverfolgungsbehörden ohne sein Wissen ein Programm zugespielt bzw. unmittelbar auf seinem PC installiert wird, das die Festplatte nach bestimmten Daten durchsuchen und diese dann bei einer Verbindung mit dem Internet den Strafverfolgungsbehörden zuspielen soll. Hinzu kommt aber wohl auch, dass die Diskussion um die Online-Durchsuchung in vielerlei Hinsicht typisch für neue Ermittlungsmethoden im Zusammenhang mit der Nutzung der Informationstechnologie ist und – in einer Zeit, in der

[1] Vgl. etwa *Bär*, MMR 2007, 239 ff.; *Buermeyer*, RS 2007, 154 ff.; *Cornelius*, JZ 2007, 798 ff.; *Hamm*, NJW 2007, 932 f.; *Kemper*, ZRP 2007, 105 ff.; *Kudlich*, JA 2007, 391 ff.; *Kutscha*, NJW 2007, 1169 ff.; *Valerius*, JR 2007, 275 ff.; *Warntjen*, Jura 2007, 581 ff.; außerdem auch zur Entscheidung des Ermittlungsrichters, z.B. *Jahn/Kudlich*, JR 2007, 57 ff.

[2] Vgl. nur die Darstellungen auf http://www.spiegel.de/politik/deutschland/0,1518,464987,00.html; http://www.spiegel.de/netzwelt/web/0,1518,464405,00.html; http://www.heise.de/newsticker/meldung/84813; http://www.zeit.de/online/2007/29/BKA-Gesetz?from=rss; http://www.focus.de/politik/deutschland/online-durchsuchung_aid_65026.html (alle zuletzt abgerufen am 18.09.2007).

[3] Im Folgenden wird zu zeigen sein, dass dieses Gefühl auch nicht trügt!

etwa auch intensiv über die Vorratsdatenspeicherung diskutiert wird – die Ängste des Bürgers vor seiner „Vergläserung“ geschürt werden.

2 Als solche Typika sind insbesondere zu nennen:

3 - Das Vorliegen neuer und ungeklärter Rechtsfragen, die eine spontane Einschätzung schwierig machen, ob eine bestimmte Ermittlungsmaßnahme zulässig ist oder nicht.[4]

4 - Der durchaus offensive Umgang der Strafverfolgungsbehörden mit den mehr oder weniger „entwicklungsoffenen“ strafprozessualen Ermittlungsbefugnissen (und letztlich auch mit den soeben genannten bestehenden Unklarheiten) dahingehend, dass Maßnahmen, die technisch möglich sind, offenbar erst einmal in der Hoffnung beantragt werden, der Ermittlungsrichter werde diese schon genehmigen.

5 - Die schwierige (insbesondere auch grund-) rechtliche Zuordenbarkeit von Ermittlungsmaßnahmen im Zusammenhang mit dem durch eine Konvergenz der klassischen Medienkommunikationsformen geprägten Internet.

6 Im Folgenden soll zunächst die Entscheidung des Ermittlungsrichters des BGH bzw. des 3. Strafsenats nachgezeichnet und kritisch gewürdigt werden (sogleich II.), bevor wichtige Gesichtspunkte für eine eventuelle Einführung einer Befugnisnorm zur verdeckten Online-Durchsuchung *de lege ferenda* skizziert werden (im Anschluss III.).

S. 203

7 II. Unzulässigkeit verdeckter Online-Durchsuchungen de lege lata

1. Der Ermittlungsrichter des BGH hat – auch auf die Beschwerde der Generalbundesanwaltschaft hin – die Anordnung einer verdeckten Online-Durchsuchung abgelehnt. Diese Entscheidung wurde vom 3. Strafsenat im Beschwerdeverfahren bestätigt. Trotz eines durchaus nachvollziehbaren kriminaltaktischen Interesses an solchen Maßnahmen[5] und ungeachtet der Bewertung einer Online-Durchsuchung als zulässig durch Teile der Literatur und auch in einer früheren Entscheidung eines anderen Ermittlungsrichters des BGH[6] ist dieser ablehnenden Haltung im Ergebnis eindeutig zuzustimmen. Dabei kommt es auf die Frage der erheblichen Eingriffsintensität und der verfassungsrechtlichen Rechtfertigung noch gar nicht entscheidend an, da es schlechterdings an einer aufgrund des Vorbehalts des Gesetzes unverzichtbaren Befugnisnorm für den – als solchen unbestrittenen – Grundrechtseingriff fehlt:

8 Es handelt sich bei der „verdeckten Online-Durchsuchung“ eben um keine Durchsuchung im Sinn der Strafprozessordnung, da eine solche – das ergibt sich etwa aus den §§ 106, 107, StPO aber auch § 110c StPO[7]– grundsätzlich ein „offenes“ Tätigwerden der Strafverfolgungsbehörden vor Augen hat. Aus den Erstgenannten, soweit etwa die Hinzuziehung des Inhabers oder die Übergabe eines Sicherstellungsverzeichnisses angeordnet wird, aus der Vorschrift über den Einsatz Verdeckter Ermittler, da auch diese Wohnungen, die nicht allgemein zugänglich sind (vgl. § 110b II Nr. 2 StPO), nur mit dem Einverständnis des Berechtigten betreten dürfen und somit – wenn schon das nur heimliche Betreten einer Wohnung untersagt ist[8] – noch viel mehr auch deren heimliche Durchsuchung unzulässig sein muss.

---

[4] Umfassender – und bis heute im Wesentlichen aktueller – Überblick bei *Böckenförde*, Die Ermittlung im Netz (2003). Bezeichnend für die Unklarheiten bzw. Schwierigkeiten die – im Zusammenhang mit der Weite des Schutzbereiches des Art. 10 GG für Telekommunikationsverbindungsdaten – kurz hintereinander ergangenen, sich fast diametral entgegenstehenden Entscheidungen der 3. Kammer des 2. Senats (BVerfG NJW 2005, 1637 m. Anm. *Kudlich*, JA 2006, 88) der sowie des 2. Senats des BVerfG selbst (in der „Bargatzky-Entscheidung“, NJW 2006, 976 m. Anm. *Jahn*, JuS 2006, 491).

[5] Gerade bei organisiert vorgehenden Straftätern liegt das Interesse auf der Hand, einerseits möglichst zeitnah auf bestimmte Daten zugreifen zu können, andererseits den Rest der Organisation nicht durch einen offenen Zugriff im Wege einer traditionellen Durchsuchung und Beschlagnahme zu warnen.

[6] Vgl. StV 2007, 60 m. Anm. *Beulke/Meininghaus*; *Hofmann*, NStZ 2005, 121, 123 ff.

[7] Vgl. zur Begründung näher *Jahn/Kudlich*, JR 2007, 57, 59.

[8] Vgl. nur *Meyer-Goßner*, 50. Aufl. (2007), § 110c StPO Rn. 1 a.E.

S. 204

9 2. Ebenso zutreffend ist, wenn der BGH insoweit auch eine analoge Anwendung der §§ 102, 105 I StPO ausschließt.[9] Solche Analogien werden zwar von der h.M.[10] wegen der von ihr befürworteten Unanwendbarkeit des Art. 103 II GG auf den Regelungsgegenstand des Strafprozessrechts in gewissen Grenzen gestattet.[11] Grenzen sind dem jedoch durch das in Art. 20 III GG wurzelnde Prinzip vom Vorbehalt des Gesetzes gesetzt.[12] Dabei handelt es sich bei der Online-Durchsuchung um eine derart grundrechtswesentliche Maßnahme, dass sie nur durch den parlamentarischen Gesetzgeber gestattet werden darf. Es ist daher unzulässig, wenn die Richter „einzelne Elemente geschriebener Erlaubnisnormen baukastenartig kombinieren und sich selbst eine Erlaubnisregel für eine einheitliche Ermittlungsmaßnahme auf einem neuen technischen Standard zusammensetzen“[13].

10 3. Zuletzt ist auch weder ein Rückgriff auf § 100a StPO noch auf die 1999 eingefügte strafprozessuale Ermittlungsgeneralklausel der §§ 161 I S. 1, 163 I StPO möglich. Eine Überwachung der Telekommunikation wird aus diesem Eingriff nicht etwa schon deswegen, weil der Zugriff nur jeweils dann möglich ist, wenn der Verdächtige „online“ ist[14]. Zwar mögen Telekommunikationsvorgänge bei der Computerausforschung tangiert sein, die Maßnahme zielt aber gerade weiter auf eine viel umfassendere Erhebung von Informationen ab. Insoweit unterscheidet sich die Situation maßgeblich von der bekannten „Mailbox-Entscheidung“ des Ermittlungsrichters des BGH.[15] Die strafprozessuale Generalklausel ermöglicht – unabhängig vom Schutzbereich des Art. 13 I GG (vgl. u.) – keinesfalls einen derart tiefgehenden Eingriff auch nur in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 I i.V.m. Art. 1 I GG)[16].

S. 205

11 ## III. Möglichkeiten und Grenzen einer verdeckten Online-Durchsuchung de lege ferenda

Neben entschiedenen Befürwortern einer Einführung der Möglichkeit einer Online-Durchsuchung etwa durch den Bundesinnenminister und das BKA ist auf politischer Ebene gegenwärtig noch ein erheblicher Widerstand festzustellen. Die Demarkationslinie zieht sich quer durch die große Koalition, und insbesondere die – für den Bereich der Strafverfolgung primär zuständige – Justizministerin hegt große Bedenken.[17] Dennoch

[9] Vgl. zum Folgenden auch bereits *Jahn/Kudlich*, JR 2007, 57, 59 f.

[10] *Meyer-Goßner* (Fn. 8), Einl. Rn. 198 ff.; *Bär*, Der Zugriff auf Computerdaten im Strafverfahren (1992), S. 51 ff.

[11] Kritisch aber etwa *Lüderssen/Jahn* in: Löwe/Rosenberg, 26. Aufl. (2006), Einl. M Rn. 47. Jedenfalls für das ebenfalls in Art. 103 II GG wurzelnde Rückwirkungsverbot hat das BVerfG (E 113, 273 [301 f.] m. insoweit zust. Anm. *Ranft*, wistra 2005, 361 [364 f.]) in der Entscheidung zum europäischen Haftbefehl – wenn auch den Nichtigkeitsausspruch nicht tragend – ausdrücklich anerkannt, dass es auch im Prozessrecht Lagen geben kann, die eine Anwendung des Art. 103 II GG rechtfertigen.

[12] Vgl. *Kudlich*, Strafprozeß und allgemeines Mißbrauchsverbot, 1998, S. 141 ff.

[13] *Weiler*, Gedächtnisschr. f. Meurer, 2002, 395 (402). Ebenso *Gornig*, in: v.Mangoldt/Klein/Starck 5. Aufl. (2007), Art. 13 Rdnrn. 65 f.

[14] In diese Richtung (letztlich aber dennoch auf §§ 102, 105 StPO abstellend) *Hofmann*, NStZ 2005, 121 (122).

[15] BGH (ER) NStZ 1997, 247 (248) m. Anm. *Kudlich*, JuS 1998, 209. Schon damals wurde im Übrigen betont, dass aufgrund der Nähe zu einer Durchsuchungsmaßnahme zusätzlich die Voraussetzungen des § 103 I 1 StPO einzuhalten seien.

[16] Vgl. *Rogall*, Informationseingriff und Gesetzesvorbehalt im Strafprozessrecht, 1992, S. 74 ff.; *Hofmann*, NStZ 2005, 121. Zu der dieser Differenzierung zugrunde liegenden „Schwellentheorie“ vgl. *Hilger*, Festschr. f. Rieß, 2002, 171, 181; *Roxin*, Strafverfahrensrecht, 25. Aufl. (1998), § 10 Rn. 17. Zum Anwendungsbereich der Ermittlungsgeneralklausel im Online-Bereich auch *Böckenförde* (Fn. 4), S. 152 ff.

[17] In der gegenwärtigen Diskussion in den Medien, aber wohl auch innerhalb der Politik selbst wird dabei oft nicht ganz klar zwischen dem präventiven und dem strafprozessualen Bereich unterschieden. Die vorliegende Untersuchung bezieht sich dabei praktisch ausschließlich auf die Frage nach einer strafprozessualen Online-Durchsuchung. Freilich sind im Unterschied zu den Ausführungen unter II. die nachfolgenden verfassungsrechtlichen Erwägungen unter III. zumindest teilweise durchaus übertragbar, und gerade in von der Problematik der verdeckten Online-Durchsuchung wohl besonders betroffenen Kriminalitätsbereichen wie der organisierten Kriminalität und terroristischen Aktivitäten ist die Grenze zwischen Prävention und Repression ohnehin durchlässiger als in vielen anderen Kriminalitätsbereichen.

spricht eine gewisse Wahrscheinlichkeit dafür, dass – nicht zuletzt auch aufgrund der politischen Signalwirkung der Anfang September erfolgten Enttarnung terroristischer Attentäter – auch eine Regelung über die strafprozessuale verdeckte Online-Durchsuchung kommen wird, wenngleich diese sich noch nicht im aktuellen Gesetzentwurf zur „Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“[18] findet. Überlegungen dazu, wie eine solche Befugnisnorm im Einzelnen aussehen könnte, sind naturgemäß Spekulation; auch würde es den vorliegenden Rahmen sprengen, einen im Detail ausgearbeiteten und begründeten Regelungsvorschlag zu machen. Vielmehr sollen im Folgenden einige Aspekte schlaglichtartig aufgegriffen werden, die in der bisherigen Diskussion um die verdeckte Online-Durchsuchung aufgeworfen sind:

12 **1. Notwendigkeit einer Verfassungsänderung?**

a) Ungeachtet aller politischen und regelungstechnischen Probleme im Einzelnen wäre die Schaffung einer entsprechenden Befugnisnorm für den Gesetzgeber selbstverständlich möglich. Fraglich ist dabei jedoch, ob damit zugleich eine Verfassungsänderung einhergehen muss. Soweit die von einer verdeckten Online-Durchsuchung möglicherweise betroffenen Grundrechte ohnehin mit einem allgemeinen Gesetzesvorbehalt versehen sind, wäre dies nicht erforderlich, und die gesetzliche Neuregelung müsste „nur“ materiellrechtlich verfassungsgemäß bleiben. Von besonderem Interesse ist daher, ob – neben anderen bzw. sogar vorrangig – auch Art. 13 GG betroffen sein könnte, da dieser keinen allgemeinen Gesetzesvorbehalt enthält, sondern eine ausdifferenzierte Schrankendogmatik, welche einen verdeckten Online-Zugriff zu strafprozessualen Zwecken nicht decken würde.[19] Dies gibt der Frage nach dem Vorliegen eines Eingriffs in den Schutzbereich der Unverletzlichkeit der Wohnung durch eine Online-Durchsuchung ihre besondere Brisanz.

S. 206

13 Das Problem, inwiefern durch eine strafprozessuale Ermittlungsmaßnahme in Computernetzen auch die Unverletzlichkeit der Wohnung berührt ist, ist schon relativ alt. Bereits vor rund zehn Jahren trat dieses Problem im Zusammenhang mit dem heimlichen Zugriff auf in einer Mailbox abgelegten Daten auf, bei dem in der Literatur teilweise ein entsprechender Eingriff in Art. 13 GG bejaht worden ist. Während dies für den damals zu entscheidenden Sachverhalt fraglich war, da der Betreiber der Mailbox generalisierend betrachtet grundsätzlich mit einem Zugriff durch den Inhaber eines Passwortes einverstanden gewesen sein dürfte, spricht bei der verdeckten Online-Durchsuchung im Ergebnis jedenfalls dann viel für die Einschlägigkeit von Art. 13 GG, wenn sich der durchsuchte Rechner in der räumlichen Schutzsphäre dieses Grundrechts befindet.[20]

14 Das Grundrecht auf Unverletztheit der Wohnung aus Art. 13 GG verbürgt dem Einzelnen einen elementaren Lebensraum und gewährleistet das Recht, in diesem Raum in Ruhe gelassen zu werden.[21] Es enthält damit das an die öffentliche Gewalt gerichtete Verbot, gegen den Willen des Wohnungsinhabers in die Wohnung einzudringen, nach der Rechtsprechung des Bundesverfassungsgerichts aber auch das grundsätzliche Verbot, etwa Abhörgeräte in der Wohnung zu installieren. Dieses Verbot schützt aber nicht nur gegen die unerwünschte physische Anwesenheit eines Vertreters der Staatsgewalt, da die heutigen technischen Möglichkeiten es erlauben, in die geschützte räumliche Sphäre auch anders einzudringen.[22] Der Schutzzweck des Grundrechts würde vereitelt, wenn der Schutz vor einer Überwachung der Wohnung durch technische Hilfsmittel nicht umfasst wäre, nur weil sie außerhalb der Wohnung eingesetzt werden.

---

[18] Vgl. BT-Drs. 16/5846 vom 27.06.2007.
[19] Vgl. bereits knapp *Jahn/Kudlich*, JR 2007, 57, 60; näher etwa *Hornung*, JZ 2007, 828 ff. (der überzeugend – gegen *Rux*, JZ 2007, 285 ff. – auch eine analoge Anwendung der Absätze 2 ff. des Art. 13 GG ablehnt).
[20] Gegen eine solche Differenzierung (und daher den Schutz durch Art. 13 GG im Ergebnis ablehnend) *Beulke/Meininghaus*, StV 2007, 63, 54.
[21] Vgl. nur BVerfGE 32, 54, 75; BVerfGE 76, 83, 89 f.; BVerfGE 109, 279, 309.
[22] Vgl. BVerfGE 109, 279, 309.

15 Zwar wird von einer verbreiteten Meinung die Einschlägigkeit des Art. 13 GG bei der Online-Durchsuchung verneint,[23] da es Zweck des Grundrechts auf Unverletzlichkeit der Wohnung sei, den Staat aus der Wohnung, nicht aber „aus dem Rechner" herauszuhalten. Auch führe der Anschluss eines Rechners an das Internet dazu, dass – wenn schon keine subjektive Einwilligung,[24] so doch jedenfalls – eine Änderung der „objektiven Kommunikationsbedingungen" dergestalt eintrete, dass diese nunmehr gewissermaßen „offen" würden. Trotz der räumlichen Abschottung der Wohnung könne jetzt mit dem Computer mit der Außenwelt kommuniziert wie umgekehrt aus dem Netz grundsätzlich auf den Computer zugriffen werden. Mit dem Anschluss an das Internet entstehe also ein gegenüber der Wohnung eigenständiger „virtueller Raum". Sobald man „online gehe", könne man auf den Schutz des Wohnungsgrundrechts nicht länger vertrauen; die durch firewalls oder sonstige Vorkehrungen geschaffenen „virtuellen Räume" würden dagegen nicht in den Schutzbereich des Art. 13 GG fallen.

S. 207

16 Richtigerweise ist demgegenüber davon auszugehen, dass der Schutzbereich des Art. 13 GG jedenfalls dann betroffen ist, wenn der von der Online-Durchsuchung betroffene Rechner in einer Wohnung steht.[25] Das Argument der angeblichen „Öffnung der objektiven Kommunikationsbedingungen" durch den Anschluss an das Internet ist wenig überzeugend. Zum einen ist schon nicht zu vermitteln, warum eine solche „virtuelle Öffnung" von Bedeutung, ein „virtueller Raum" kraft firewalls etc. dagegen unbeachtlich sein soll. Vor allem aber wird auch sonst durch eine Öffnung der Wohnung gegenüber solchen Personen, die *mit Wissen und Wollen* des Wohnungsinhabers eintreten, der räumliche Schutz *im Übrigen* nicht tangiert.

17 Vielmehr muss Art. 13 GG auch die Verfügungsbefugnis darüber schützen, welche Informationen aus der Wohnung eigenmächtig „entnommen" werden. Mit Blick auf die (eingangs auch schon knapp skizzierte) vielfach überragende Bedeutung der vielfältigen, auf einem Rechner gespeicherten Daten, kann ihr „Entziehen" aus der Wohnung nicht als weniger schwerwiegend erachtet werden als das Entnehmen körperlicher Gegenstände, der Einblick in visuell wahrnehmbare Gegebenheiten oder das Abhören des „im Vertrauen auf den Schutzbereich der Wohnung und seine Flüchtigkeit gesprochenen Wortes"[26]. Anders als von der Gegenmeinung propagiert, stellt die Wohnung eben dennoch eine zusätzliche räumliche Abschottung dar. Zwar ist es im Einzelfall ohne Zweifel Zufall, ob der Nutzer innerhalb oder außerhalb seiner Wohnung (etwa in einem Internetcafe oder an einem Hot Spot) „online geht" – diese Zufälligkeit spricht aber nicht gegen eine Einbeziehung in den grundrechtlichen Schutzbereich. Vielmehr ist es bei allen Gegenständen in diesem Sinne vom Zufall abhängig, ob sie sich in einer Wohnung befinden (und dem Zugriff darauf dann unter Umständen Art. 13 GG entgegensteht) oder außerhalb der Wohnung. Auch die Ungewissheit der Strafverfolgungsbehörden darüber, ob sie in eine Wohnung eindringen, bzw. die insoweit fehlende Finalität im engsten Wortsinne[27] ändern daran nichts. Wie *Hornung* überzeugend ausführt, muss eben eine staatliche Stelle, wenn sie „bei ihrem Handeln (…) nicht genau weiß, ob sie

[23] Vgl. etwa – teilweise noch vor der aktuellen Diskussion – *Germann*, Gefahrenabwehr und Strafverfolgung im Internet (2000), S. 540 ff.; *Gercke*, CR 2007, 245, 250; *Graf*, DRiZ 1999, 281, 285; *Hofmann*, NStZ 2005, 121, 124; *Perrey*, Gefahrenabwehr und Internet (2003), S. 128; im Ergebnis auch *Beulke/Meinighaus*, StV 2007, 63, 64. In der gegenwärtigen politischen Diskussion sind es insbesondere die Befürworter einer raschen Einführung einer entsprechenden gesetzlichen Regelung in Unionskreisen, die offenbar von der Nicht-Einschlägigkeit von Art. 13 GG ausgehen.

[24] In diese Richtung denkend aber offenbar *Hofmann*, NStZ 2005, 121, 124.

[25] Insoweit im Ergebnis ebenso *Hornung*, JZ 2007, 828, 831; *Rux*, JZ 2007, 285 ff.; a.A. etwa Meininghaus, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren (2007), S. 146 ff., 257.

[26] Anders insoweit *Hofmann*, NStZ 2005, 121, 124.

[27] Nämlich so verstanden, dass der Rechner ebenso gerne „online-durchsucht" würde, wenn er sich nicht in einer Wohnung befinden würde – aber auch das ist an sich keine Besonderheit: Auch Aktenordner in einem Wirtschaftsstrafverfahren werden die Strafverfolgungsbehörden ebenso gerne an sich nehmen, unabhängig davon, ob sie sich in einer Wohnung oder etwa im Auto des Beschuldigten befinden; das ändert aber nichts daran, dass ein Eingriff in den Schutzbereich des Art. 13 GG vorliegt, *wenn* die Akten aus der Wohnung getragen werden.

in ein bestimmtes Grundrecht (…) eingreift, im konkreten Fall jedoch typischerweise damit rechnen muss, (…) die insoweit bestehenden verfassungsrechtlichen oder einfachgesetzlichen Eingriffsvoraussetzungen ein(zu)halten. Dies gilt sowohl für die Verwaltung bei der Entscheidung über eine Einzelmaßnahme, als auch für den Gesetzgeber."[28]

18 b) Wird entgegen der hier vertretenen Ansicht die Einschlägigkeit von Art. 13 GG abgelehnt, wäre die Einführung einer entsprechenden strafprozessualen Befugnisnorm auch ohne Verfassungsänderung möglich. Das Fernmeldegeheimnis nach Art. 10 GG ist nach überzeugender Ansicht ohnehin nicht – bzw. zumindest nicht grundsätzlich – von der Online-Durchsuchung tangiert, da dies von vornherein nur bei Dokumenten denkbar wäre, die über einen Kommunikationsvorgang erhalten worden sind (insbesondere E-Mails), und auch hier wohl nur, solange der Kommunikationsvorgang noch nicht abgeschlossen ist;[29] außerdem würde das Fernmeldegeheimnis in Art. 10 II 1 GG ohnehin einen hinreichend weit formulierten Gesetzesvorbehalt enthalten. Dies gilt erst recht für den – auch von denjenigen, die einen Eingriff in den Schutzbereich des Art. 13 GG ablehnen, zugestandenen – Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 I, 1 I GG (welcher – nebenbei bemerkt – die zweifelhafte Ablehnung des Schutzbereiches von Art. 13 GG nicht zu „kompensieren" vermag, da durch eine Gleichsetzung dieses Eingriffs etwa mit der Videoüberwachung öffentlicher Plätze eine völlig unangemessene Bagatellisierung einhergehen würde).

S. 208

19 **2. Materielle Verfassungsmäßigkeit**

Auch wenn unter formell verfassungsrechtlichen Gründen keine Schaffung eines weiteren Gesetzesvorbehaltes erforderlich sein oder aber eine solche erfolgen sollte, bleiben Zweifel an der materiellen Verfassungsmäßigkeit einer entsprechenden Regelung. Diese nähren sich zum einen aus dem Verhältnis von besonderer Eingriffsintensität und zweifelhaftem Nutzen der Maßnahme, zum anderen auch aus der Schwierigkeit bei der Gestaltung eines hinreichenden Schutzes des Kernbereichs der privaten Lebensgestaltung, welche verfassungsrechtlich geboten wäre:

20 a) Die Eingriffsintensität einer verdeckten Online-Durchsuchung wäre ganz erheblich: Dies rührt zum einen aus den vielfältigen davon potentiell betroffenen Daten her, welche zahlreiche – und mitunter auch besonders sensible – Lebensbereiche betreffen[30] und die aus unterschiedlichsten Quellen beim Nutzer gelandet sein können. So finden sich auf einem PC gerade nicht nur Dokumente, die der Nutzer selbst erstellt hat, sondern u.U. auch solche, die Gegenstand einer von Art. 10 GG geschützten Kommunikation (etwa via E-Mail) gewesen sind. Nach der neueren Rechtsprechung des Bundesverfassungsgerichts genießen solche Dokumente nach Abschluss des Kommunikationsvorganges zwar nicht mehr den Schutz von Art. 10 GG[31]; es wird jedoch deutlich, dass verschiedenste Inhalte aus unterschiedlichsten Quellen den gesamten Bereich der Lebensgestaltung betreffen können.

21 Hinzu kommt das Element der Heimlichkeit.[32] Die StPO zeigt an den verschiedensten Stellen (etwa bei der Überwachung der Telekommunikation, beim Einsatz von verdeckten Ermittlern oder beim kleinen und erst recht großen Lauschangriff), dass nichtoffene Ermittlungsmethoden – selbst wenn man diese nicht als der StPO grundsätzlich wesensfremd bewertet – über eine besondere Eingriffsintensität verfügen und daher nur im Zusammenhang mit besonderen materiellen (z.B. Katalogtaten, Subsidiaritäts-

[28] Vgl. *Hornung*, JZ 2007, 828, 830.
[29] Das gilt jedenfalls nach der neueren Rechtsprechung des BVerfG, vgl. nochmals BVerfG NJW 2006, 976.
[30] Also etwa im Zusammenhang mit Schreiben an das Finanzamt oder die Krankenkasse Einkommens- und Gesundheitsverhältnisse ebenso wie z.B. tagebuchartige Aufzeichnungen.
[31] Vgl. nochmals Fn. 29.
[32] Für eine offene Online-Durchsuchung nimmt *Valerius*, JR 2007, 275, 278, sogar an, dass diese schon de lege lata zulässig wäre.

klausel) und formellen (Richterzuständigkeit) Sicherungen möglich sind.

S. 209

22 Im Unterschied zu einer „traditionellen Durchsuchung“ enthält die verdeckte Online-Durchsuchung aber auch noch ein zusätzliches Element der verlängerten Dauer des Eingriffs, welches für den Zeitraum, währenddessen sich die Software auf dem Rechner befindet, Elemente einer „Echt-Zeit-Überwachung“ besitzt. Während bei einer traditionellen, offenen Durchsuchung nur die Inhalte einer Wohnung speziell zum Zeitpunkt der Untersuchung aufgefunden werden können, ändern sich die Inhalte auf dem PC möglicherweise während der Dauer der Maßnahme.[33]

23 b) Dieser massiven, durch inhaltliche Breite und Kombination der Elemente verschiedener anderer Maßnahmen geprägten Eingriffsintensität könnte auf der anderen Seite ein begrenzter Nutzen bzw. eine begrenzte Anwendbarkeit der Befugnisnorm entgegenstehen. Selbst das BKA spricht davon, dass die Online-Durchsuchung jährlich nur in rund zehn Fällen angewendet würde, da sie auf besonders schwere Kriminalitätsformen beschränkt bleiben solle und einen erheblichen Vorbereitungsaufwand mit sich bringe. Auch wird – wobei man zugegebenermaßen über die technischen Details im Dunkeln tappt – von verschiedener Seite bezweifelt, ob diese Maßnahmen überhaupt wirkungsvoll eingesetzt werden können, wenn der Beschuldigte etwa über eine gut gepflegte firewall verfügt.

24 c) Allerdings darf der Gesichtspunkt der voraussichtlich seltenen Anwendung einer entsprechenden Maßnahme sowie des daraus dann – auf einer „Makroebene“ betrachtet – resultierenden beschränkten Nutzens im Rahmen der Verhältnismäßigkeitsprüfung nicht entscheidend als vermeintliches Argument gegen die Effektivität der Maßnahme und daher letztlich gegen ihre Angemessenheit herangezogen werden. Vielmehr ist die Beschränkung auf wenige Fälle schwerster Kriminalität ja gerade eine Ausprägung des Verhältnismäßigkeitsgrundsatzes oder anders gewendet: Es liegt eine unzulässige Vermischung der verschiedenen Perspektiven vor, wenn man bei der Eingriffsschwere auf die „Mikroebene“ des konkret betroffenen einzelnen Beschuldigten abstellt, bei der „Makroebene“ dagegen auf die geringe Zahl der Fälle, in denen die Maßnahme voraussichtlich Anwendung finden wird. Dass ein solcher Perspektivenwechsel nicht zu sinnvollen Ergebnissen führen kann, wird schon daraus deutlich, dass man ihn genauso gut in umgekehrter Weise durchführen könnte: Dann stünden auf der „Makroebene“ geringe (da seltene) Eingriffe im Raum, denen im Einzelfall möglicherweise ein großer Ermittlungsnutzen gegenüberstehen würde.

S. 210

25 d) Lässt sich also aus der Gegenüberstellung der – zugegebenermaßen großen – Intensität des Eingriffs und seines Nutzens letztlich keine vernünftige Aussage über die materielle Verfassungsmäßigkeit einer entsprechenden Befugnisnorm treffen, so kann – nicht zuletzt auch aufgrund der erheblichen Einschätzungsprärogative des Gesetzgebers hinsichtlich der Erforderlichkeit und damit zumindest teilweise auch der Angemessenheit einer Maßnahme – eine belastbare Aussage nur durch einen „schweren Vergleich“ mit anderen, bereits im Gesetz vorgesehenen Maßnahmen getroffen werden. Ein solcher, gleichsam nur systemimmanenter und nicht systemtranszendenter Vergleichsmaßstab hat zwar den unbestrittenen Nachteil, dass er nur teilweise „autonome“ verfassungsrechtliche Bewertungen enthält. Aus praktischer Sicht ist jedoch zu berücksichtigen, dass die – zu weiten Teilen jedenfalls in der gegenwärtigen Gesetzesfassung bejahte – grundsätzliche Verfassungsmäßigkeit der strafprozessualen Ermittlungsbefugnisse einerseits und die vom Verfassungsgericht gezogenen Grenzen andererseits einen brauchbaren Rahmen für eine insoweit zumindest „abgeleitete“ verfassungsrechtliche Beurteilung bilden.

26 Stellt man nun einen solchen Vergleich an, so ist zunächst festzustellen, dass die ver-

[33] Vgl. *Kudlich*, JA 2007, 391, 393.

deckte Online-Durchsuchung trotz ihrer Neuartigkeit hinsichtlich ihrer Einzelelemente *keine generelle neue Qualität* besitzen würde: So ist bereits seit langer Zeit der Zugriff auf Computerdaten – sei es durch eine Beschlagnahme nach §§ 94 ff. StPO[34], sei es auch bei der Überwachung der elektronischen Kommunikation mit Hilfe moderner Informationstechnologien nach §§ 100a ff. StPO[35] - im Strafverfahren mehr oder weniger tägliche Praxis.[36] Der verdeckte Charakter von Maßnahmen ist ebenfalls Bestandteil einer Reihe strafprozessualer Ermittlungsbefugnisse und dabei insbesondere auch der – mit der Online-Durchsuchung zumindest hinsichtlich der technischen Abläufe gewisse Gemeinsamkeiten bildenden – Überwachung der Telekommunikation. Die Möglichkeit schließlich, dass durch eine prozessuale Ermittlungsmaßnahme auf mehr oder weniger vertrauliche Daten zugegriffen wird, besteht grundsätzlich bei fast jeder strafprozessualen Untersuchungshandlung und ist bereits im Kernbestand der StPO etwa in Gestalt der Beschlagnahmeverbote zumindest partiell berücksichtigt und bildet in § 100c StPO geradezu den Grund für eine umfangreiche gesetzliche Regelung.

27 Anders gewendet: Die verdeckte Online-Durchsuchung bildet weniger hinsichtlich ihrer einzelnen Elemente als vielmehr hinsichtlich der Kombination dieser Elemente miteinander und hinsichtlich der erzielbaren Datenmenge ein Novum. Wo es indes stärker um die *Quantität* als um eine etwaige neuartige *Qualität* der Grundrechtseingriffe geht, spricht vieles dafür, dass sich eine Regelung finden lassen würde, die in das bestehende Regelungssystem in einer verfassungsrechtlich zulässigen Weise eingepasst werden könnte. Notwendig wäre – nur, aber immerhin –, dass die durch die Summierung und Kombination von Belastungen entstehende Eingriffsintensität in materieller wie formeller Hinsicht hinreichend abgefedert wird. Vorstellbar sind hier etwa die Beschränkung auf Straftatenkataloge (welche dann nicht die mittlerweile fast schon beliebige Weite des § 100a StPO bekommen dürften) sowie eine etwa § 100d I StPO vergleichbare oder sogar „noch höher aufgehängte" Zuständigkeitsregel. Flankierende Maßnahmen wie Vernichtungs- und Dokumentationspflichten in § 100d V StPO wären ebenfalls unverzichtbar.

28 Zusammengefasst erscheint daher die Einführung einer strafprozessualen Befugnisnorm zur verdeckten Online-Ermittlung zwar rechtspolitisch nicht unbedingt wünschenswert, da den intensiven Grundrechtseingriffen nur ein beschränkter Anwendungsbereich gegenübersteht und überdies auch bei einer Datensammlung in diesem Umfang die Missbrauchsgefahr – nicht durch die Strafverfolgungsbehörden, sondern durch Dritte, die in den Besitz der Daten gelangen – erheblich sein kann.[37] Eine generelle materielle Verfassungswidrigkeit einer entsprechend sorgfältig formulierten Regelung scheint aber nicht prognostizierbar.[38]

S. 211

29 ### 3. Kernbereich der privaten Lebensgestaltung

Wie auch bei anderen Ermittlungsmaßnahmen wäre dabei allerdings auch bzw. sogar gerade bei der verdeckten Online-Ermittlung dafür Sorge zu tragen, dass der vom Bundesverfassungsgericht in der Entscheidung BVerfGE 109, 279, 309, 312 ff. geforderte Schutz des Kernbereichs der privaten Lebensgestaltung berücksichtigt wird. Dass dieses – vom Gesetzgeber etwa auch in den gegenwärtigen Reformüberlegungen zur Überwachung der Telekommunikation aufgegriffene – Anliegen selbstverständlich auch

[34] Vgl. zu den damit zusammenhängenden Problemen ausführlich *Böckenförde* (Fn. 4), S. 257 ff., insb. 336 ff..
[35] Vgl. zu den damit zusammenhängenden Problemen ausführlich *Böckenförde* (Fn. 4), S. 417 ff.; speziell im Zusammenhang mit dem Zugriff auf E-Mails auch *Valerius*, Ermittlungen der Strafverfolgungsbehörden in den Kommunikationsdiensten des Internet (2004), insb. S. 90 ff, sowie Meininghaus, Der Zugriff auf E-Mails im strafrechtlichen Ermittlungsverfahren (2007), passim.
[36] Grundlegend (damals im Wesentlichen noch für den „Offline-Bereich") bereits *Bär* (Fn. 10).
[37] Vgl. dazu eindringlich *Pfitzmann*, im Fachgespräch „Bürgerrechtsschutz im digitalen Zeitalter" bei der Fraktion von Bündnis 90/Die Grünen am 26.3.2007 (Dokumentation/Reader R-16-79 vom 10.07.2007 zur Tagung vom 26.03.2007), S. 10, 14, 55.
[38] Nach hier vertretener Ansicht ist dabei allerdings eine gleichzeitige Änderung von Art. 13 GG erforderlich, vgl. oben.

bei der Online-Durchsuchung eine Rolle spielt (und nicht wie bei der Gestaltung des Verfassungsschutzgesetzes des Landes Nordrhein-Westfalens vernachlässigt werden darf[39]), liegt auf der Hand. Gerade aufgrund der Konvergenz der verschiedenen Medien- und Kommunikationsformen im Internet bzw. ihrer Abbildung auf der eigenen Festplatte sind grundsätzlich nahezu alle Gestaltungen, die bei anderen Ermittlungsmaßnahmen zum Kernbereich der privaten Lebensgestaltung gerechnet werden,[40] vorstellbar. Anders gewendet: Nicht jeder Inhalt wird dadurch, dass er auf der (und sei es auch durch ein Passwort geschützten) Festplatte liegt, zu einem Teil des Kernbereichs der privaten Lebensgestaltung; nahezu alles, was zu diesem Kernbereich gehören kann, könnte sich aber auf einer Festplatte befinden.

30 Die konkrete inhaltliche Gestaltung derartiger Regelungen könnte sich – trotz mancher Kritik – etwa an den in der gegenwärtigen Reformdiskussion gemachten Regelungsvorschlägen orientieren, welche hinsichtlich des Kommunikationspartners zwischen gleichsam absoluten und relativen Persönlichkeiten der privaten Lebensgestaltung differenzieren.[41] Auch eine Anlehnung an § 100c IV, V StPO wäre – *mutatis mutandis* – vorstellbar. Die eigentliche „Hürde", die dabei überwunden werden muss, liegt darin, dass man auf die Idee kommen könnte, rein schriftliche Aufzeichnungen und Kommunikationsvorgänge könnten – anders als ein persönliches Gespräch – niemals dem Kernbereich privater Lebensgestaltung zuzurechnen sein. Damit dürfte aber wohl die Realität moderner Kommunikation verfehlt werden. Dass allein die Schriftlichkeit einem entsprechenden Grundrechtsschutz nicht entgegensteht, wird – wie oben bereits erwähnt – im Zusammenhang mit der Beschlagnahme körperlicher Gegenstände nicht zuletzt auch durch die Tagebuchfälle belegt.

S. 212

31 **4. Richtervorbehalt**

Die Anordnungskompetenz für eine solche verdeckte Online-Durchsuchung müsste selbstverständlich beim Richter liegen, wobei sich hier weniger die Frage des „ob" als vielmehr des „wo" stellt, oder anders gewendet: Aufgrund der mit einer Maßnahme nach § 100c StPO durchaus vergleichbaren Eingriffsintensität spricht viel dafür, die Anordnungszuständigkeit zumindest wie in § 100d StPO bei der Strafkammer (und nicht beim Ermittlungsrichter) anzusiedeln; je nach Inhalt des konkreten Straftatenkatalogs sowie auch mit Blick auf die prognostizierte verschwindend kleine Zahl von entsprechenden Maßnahmen mag man auch an die Zuständigkeit des Strafsenates des OLG denken.

32 Dieser grundsätzliche Richtervorbehalt dürfte letztlich auch nicht bestritten sein. Wenn Ende August/Anfang September eine entsprechende Diskussion in den Medien laut geworden ist, weil der Bundesinnenminister auch eine zumindest vorübergehende Online-Durchsuchung ohne richterlichen Beschluss für erforderlich gehalten hat,[42] so dürfte es sich um eine dem aufgeheizten Diskussionsklima ebenso wie einer defizitären Öffentlichkeitsarbeit geschuldete Missinterpretation handeln, wenn diese Äußerung mitunter so verstanden worden ist, als ob in bestimmten Fällen die verdeckte Online-Durchsuchung gleichsam „regulär" auch ohne richterlichen Beschluss möglich gemacht werden soll. Vielmehr dürfte es „nur" um die Erfassung von Eilfällen gegangen sein, in denen etwa auch nach § 100b I 2 StPO die Überwachung der Telekommunikation von der Staatsanwaltschaft angeordnet werden kann, was dann jedoch nach § 100b I 3 StPO binnen drei Tagen vom Richter bestätigt werden muss.

---

[39] Vgl. LT-Drs. (NRW) 14/2211, S. 16.

[40] Also etwa vertrauliche E-Mail-Kommunikation, die durchaus den überwachten Gesprächen bei § 100c StPO vergleichbar sein kann; tagebuchähnliche Aufzeichnungen, zu welchen seit je her bei Beschlagnahmen das Problem der Verletzung des innersten Bereiches der Privatsphäre ein Problem ist usw.

[41] Vgl. BT-Drs. 16/5846 S. 22, 25, 35 ff.

[42] Vgl. nur die Meldungen auf http://de.today.reuters.com/news/NewsArticle.aspx?type=topNews&storyID=2007-08-31T052630Z_01_HUD119544_RTRDEOC_0_DEUTSCHLAND-ONLINE-SICHERHEIT.xml; http://www.tagesschau.de/inland/meldung486964.html (alle zuletzt abgerufen am 18.09.2007).

33 Betrachtet man die Systematik entsprechender Ausnahmevorschriften, so spricht jedoch einiges dagegen, eine solche auch bei der verdeckten Online-Durchsuchung zuzulassen: Die Ausnahmen sind ersichtlich nach der Intensität des Eingriffs gestaffelt. So liegt die Anordnungszuständigkeit bei Gefahr im Verzug bei der einfachen Beschlagnahme nach § 98 I StPO nicht nur bei der Staatsanwaltschaft, sondern auch bei ihren Ermittlungspersonen; der Betroffene kann dagegen zwar nach § 98 II 2 StPO „jederzeit die richterliche Entscheidung beantragen", es findet jedoch keine automatische Überprüfung statt. Bei der Überwachung der Telekommunikation liegt die Eilzuständigkeit nur noch bei der Staatsanwaltschaft und die Anordnung tritt automatisch außer Kraft, wenn sie nicht vom Richter bestätigt wird, vgl. nochmals § 100b I StPO. In den Fällen des § 100c StPO (großer Lauschangriff) liegt die Eilzuständigkeit nach § 100d I 2 StPO sogar auch nur bei einem Richter, nämlich beim Vorsitzenden der sonst zuständigen Strafkammer.

34 Geht man nun davon aus, dass die Intensität der verdeckten Online-Durchsuchung noch über Maßnahmen nach §§ 100a, 100c StPO – wenngleich nicht qualitativ, so doch zumindest quantitativ – hinausgeht, so spricht einiges dafür, hier überhaupt keine Eilzuständigkeiten anzuerkennen. Dies gilt noch umso mehr, als selbst nach der Einschätzung von Befürwortern einer Möglichkeit der Online-Durchsuchung[43] die sinnvolle und möglichst risikoarme Durchführung einer solchen Maßnahme eine mehr oder weniger lange „Umfeldanalyse" des Betroffenen erfordert. Dass dies einerseits durchgeführt werden kann, der konkrete Antrag dann aber aufgrund einer Gefahr im Verzug mittels einer Eilkompetenz[44] angeordnet werden müsste, ist praktisch nicht vorstellbar.

S. 213

35 ## IV. Zusammenfassung

Zusammenfassend bleibt also festzustellen, dass *de lege lata* der BGH eine strafprozessuale Online-Durchsuchung zurecht abgelehnt hat. Ob die Einführung einer solchen Befugnis *de lege ferenda* – obgleich kriminaltaktisch zumindest vordergründig attraktiv – (verfassungs-) rechtspolitisch wirklich wünschenswert ist, erscheint zweifelhaft – dass eine solche Maßnahme aber geschaffen wird, dennoch nahe liegend. Sollte der Gesetzgeber diese Aufgabe angehen, ist die Balance zwischen Strafverfolgung und Grundrechtsschutz eine schwierige und ernst zu nehmende Aufgabe: Ein „Wer nichts zu verbergen hat, hat auch nichts zu befürchten"-Ansatz ist sicher nicht hilfreich und kaum geeignet, das Vertrauen der Bevölkerung in die modernen Kommunikationsmittel, aber auch in die staatliche Hoheitsgewalt zu stärken.

36 Andererseits sollte man aber auch nicht zu schwarz sehen: Die Erfahrung lehrt, dass in Deutschland mitunter grundrechtlich „auf hohem Niveau gejammert" wird. Manche Schwierigkeiten ergeben sich überhaupt erst bei dem Versuch, dem doch relativ hohen Schutzniveau durch das deutsche Grundgesetz gerecht zu werden, ohne eine an die Realitäten der modernen Kriminalität angepasste effektive Strafverfolgung von vornherein auszuschließen. Wer überall nur Gefahren und staatliche Missbräuche sieht, wird immer und an jeder Regelung ein Haar in der Suppe finden.

37 Man stelle sich nur einmal vor, im Klima eines derartigen Misstrauens müsste heute noch einmal die Frage diskutiert werden, ob – was tägliche Praxis ist – körperliche Eingriffe in Gestalt einer Blutentnahme zur Aufklärung von Bagatellstraftaten im Bereich des Straßenverkehrs angeordnet werden sollen.[45] Ein Missbrauchspotential besteht auch bei abgenommenem Blut – man denke nur an die Durchführung heimlicher flächendeckender Gentests und den Aufbau entsprechender Dateien etc. Zumindest soweit wir wissen, sind trotz der vergleichsweise langen Geschichte derartiger Blutent-

[43] Vgl. etwa die Äußerung des Präsidenten des BKA, Jörg *Ziercke*, R-16-79 (Fn. 37), S. 38 f. (Erfordernis einer eingehenden „Umfeldanalyse des Betroffenen").
[44] Welche – vgl. oben – entsprechend § 100d I StPO ohnehin nicht unterhalb der Schwelle eines Richters liegen dürfte.
[45] Beispiel von *Ziercke*, in Bündnis 90/Die Grünen, R-16-79 (Fn. 37), S. 34, 50, 51.

nahmen solche Auswüchse bisher unterblieben. Bei aller gebotenen Wachsamkeit und aller Sensibilität für drohende Grundrechtseingriffe sollten wir uns also einen letzten Rest Optimismus erhalten.

Zitierempfehlung: Hans Kudlich, HFR 19/2007, Seite