3. Psycho(patho)logisch-Normative Stufe: Einsichts- und Steuerungsfähigkeit

3.1. Zur Beeinträchtigung der Einsichtsfähigkeit sowie zum Zusammenhang zwischen der Paraphilie und der Tat gelten die Ausführungen zu den Persönlichkeitsstörungen (D.I. 3.3.1. bis 3.).

3.2. Eine forensisch relevante Beeinträchtigung der Steuerungsfähigkeit kann bei Vorliegen folgender Aspekte diskutiert werden:

- Konflikthafte Zuspitzung und emotionale Labilisierung in der Zeit vor dem Delikt mit vorbestehender und länger anhaltender triebdynamischer Ausweglosigkeit,
- Tatdurchführung auch in sozial stark kontrollierter Situation.
- Abrupter, impulshafter Tatablauf, wobei jedoch ein paraphil gestaltetes und zuvor (etwa in der Phantasie) „durchgespieltes" Szenario kein unbedingtes Ausschlusskriterium für eine Verminderung der Steuerungsfähigkeit ist, sofern dieses Szenario der (den) unter 2. diagnostizierten Paraphilie(n) entspricht und eine zunehmende Progredienz nachweisbar ist,
- Archaisch-destruktiver Ablauf mit ritualisiert wirkendem Tatablauf und Hinweisen für die Ausblendung von Außenreizen
- Konstellative Faktoren (z. B. Alkoholintoxikation, Persönlichkeitsstörung, eingeschränkte Intelligenz), die u. U. auch kumulativ eine erheblich verminderte Steuerungsfähigkeit bedingen können.

E. Ausblick

Die Ergebnisse der interdisziplinären Arbeitsgruppe haben die Teilnehmer ermutigt, auch Mindestanforderungen für die im Strafverfahren vielfältig verlangten Prognosegutachten zu beraten und zu formulieren. Diese Aufgabe soll im Verlauf des Jahres 2005 angegangen werden.

Professor Dr. Ulrich Eisenberg und Wiss. Mitarbeiter Tobias Singelnstein, Berlin

Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS"

I. Problemstellung

1. Polizeibehörden von Bund und teilweise auch Ländern sind im Rahmen strafrechtlicher Ermittlungen in den vergangenen Jahren dazu übergegangen, mittels so genannter „stiller SMS"[1] den Aufenthaltsort sowie Bewegungsbilder von Zielpersonen zu ermitteln, die Mobilfunkendgeräte (Handys) nutzen. Dabei handelt es sich einmal mehr um eine Ermittlungsmöglichkeit, die intensiv in die *Rechte* des *Betroffenen eingreift*, ohne dass der Gesetzgeber sie explizit geregelt hätte. Vielmehr folgt die *Ausweitung* von Eingriffsgrundlagen durch die *polizeiliche Praxis* der technischen Entwicklung und dem Bestreben, neue Möglichkeiten zu nutzen.

Dies wirft zum einen das Problem auf, inwieweit für die Ermittlung per "stiller SMS" überhaupt eine Rechtsgrundlage besteht. In diesem Zusammenhang ist auch auf die rechtliche Konstruktion einzugehen, mittels derer die genannte Praxis unter vorhandene Rechtsgrundlagen zu fassen versucht wird (dazu unten II.). Andererseits betrifft dies Probleme der Ausweitung von Eingriffsgrundlagen durch die Praxis und der als „endlos" anmutenden Möglichkeiten heimlicher Überwachung (dazu unten III.).

2. Technisch gesehen handelt es sich bei der „stillen SMS" um ein Signal (sog. „ping"), das von den Beamten durch ein einfaches Computer-Programm oder per Handy an eine ihnen bekannte Mobilfunk-Nummer gesandt wird. Wie bei der normalen Kommunikation in Form von Telefongesprächen oder Textnachrichten mit dem Short Message Service (SMS) wird hierbei – sofern das Handy eingeschaltet ist bzw. wird – beim Mobilfunkbetreiber ein Datensatz mit den Verbindungsdaten erzeugt. Dieser enthält neben der Rufnummer etc. auch die Information, in welche Mobilfunkzelle das Gerät momentan eingebucht ist, wo es sich also in etwa befindet.[2] Diese Daten werden den Ermittlern sodann von dem betreffenden Mobilfunkbetreiber übermittelt. Für den Besitzer des Gerätes ist dieser Vorgang nicht wahrnehmbar, weshalb vereinfachend und anschaulich von „stiller SMS" gesprochen wird.

Neben Bundeskriminalamt (BKA), Zoll und Bundesgrenzschutz (BGS) – dieser hat ein eigenes Programm hierfür entwickelt – verwenden auch verschiedene Länderpolizeien die Ermittlungsmethode der „stillen SMS".[3] Deren Vorteil sowohl gegenüber IMSI-Catcher, Observation u. ä. als auch gegenüber der bloßen Abfrage von nicht künstlich erzeugten Verbindungsdaten besteht darin, dass einerseits einfach, unmittelbar und Ressourcen sparend Aufenthaltsort und genaue Bewegungsbilder ermittelt werden können, ohne andererseits darauf angewiesen zu sein, dass die Zielperson selbst ihr Handy benutzt und so Daten erzeugt.[4] Dabei scheint die „stille SMS" weniger zum Zweck gezielter Festnahmen eingesetzt zu werden. Vielmehr dienen die gewonnenen Daten offenbar häufig

1) Bezeichnungen wie „stealth SMS", „verdeckte SMS" u. ä. werden synonym verwendet.

2) Das Mobilfunknetz ist in Zellen eingeteilt, die je nach Wohndichte einen Radius von einigen hundert Metern bis hin zu mehreren Kilometern haben. Sobald das Handy in den Bereich einer anderen Zelle gelangt, bucht es sich bei dieser ein und wickelt über sie die Kommunikation ab (zur praktischen Bedeutung dieser Daten sowie zum technischen Hintergrund vgl. etwa schon *Artkämper* Kriminalistik 1998, 202, 202 f.).

3) In Niedersachsen hat laut der Antwort der Landesregierung auf eine kleine Anfrage alleine das LKA die Methode im 1. Halbjahr 2003 in 71 Verfahren angewendet (vgl. LT-Dr 15/352, S. 2). In Berlin setzte die Polizei sie bis zum April 2003 in 99 Fällen ein (vgl. AbgH-Dr 15/10 559, S. 1). Nach einem Bericht in „Der Spiegel" vom 7. 4. 2003 soll die „stille SMS" mancher Orts „Lieblingsspielzeug jedes Dorfpolizisten" sein. In einem Gesetzentwurf der CSU zur Änderung des bayerischen Polizeiaufgabengesetzes (LT-Dr 14/12 261) findet sich im Rahmen der Einführung präventiver Telekommunikationsüberwachung eine Rechtsgrundlage, die der Begründung zufolge explizit auch die „stille SMS" erfassen soll.

4) Zwar fallen Standort-Daten auch ohne aktive Kommunikation alleine dadurch an, dass sich das eingeschaltete Handy regelmäßig beim Mobilfunknetz einbucht und so die Zelle mitteilt, in der es sich befindet. Die Abfrage dieser stand by-Daten soll nach *BGH* [ER] StV 2001, 214, 215 f. im Rahmen von § 100 a StPO auch zulässig sein (a. A. *Demko* NStZ 2004, 57 ff. mwN), so dass auf diesem Weg ebenso ein Bewegungsbild erstellt werden dürfe. Für die Ermittlungsbehörden besteht aber offenbar dennoch die praktische Notwendigkeit, Standortdaten durch aktive Kommunikation mittels „stiller SMS" zu erzeugen. Dies mag einerseits damit zusammenhängen, dass die Mobilfunkbetreiber teilweise rechtlich gegen Auskunftsersuchen bezüglich stand by-Daten vorgehen – wie in der genannten Entscheidung des *Ermittlungsrichters* beim *BGH*. Zum anderen werden die im stand by-Betrieb anfallenden Standort-Daten – anders als bei aktiver Kommunikation, bei der die Daten aus Abrechnungs- und Nachweisgründen festgehalten werden – von den Mobilfunkbetreibern nicht (automatisch) gespeichert. Zwar sind die Anbieter nach Ansicht des *BGH* im Falle einer Anordnung nach §§ 100 a, 100 b StPO dennoch verpflichtet, die Daten festzuhalten und mitzuteilen. Aus technischen Gründen ist dies jedoch offenbar nur mit zeitlicher Verzögerung und nicht online möglich (vgl. *BGH* [ER] StV 2001, 214, 215 f.), so dass die stand by-Daten im Hinblick auf eine observationsunterstützende Funktion oder zum Zweck des unmittelbaren Zugriffs an Wert verlieren. Es bleibt jedoch abzuwarten, inwieweit zukünftig eine Verpflichtung zur Speicherung solcher Daten normiert werden wird; vgl. hierzu *Thiede* Kriminalistik 2004, 104, 105 ff. sowie den Gesetzentwurf zur Neuregelung des TKG (BR-Dr 755/03).

als Grundlage für weitere Ermittlungen sowie als Unterstützung bei Observationen u. ä.[5] So wird die Methode ganz überwiegend bis ausschließlich in Verfahren verwendet, in denen bereits eine Anordnung nach §§ 100 a, 100 b StPO getroffen wurde.[6]

II. Zur Frage einer einschlägig geeigneten Rechtsgrundlage

Da für die „stille SMS" im Gegensatz zu anderen Ermittlungsmethoden in diesem eingriffsintensiven Bereich[7] keine explizite Rechtsgrundlage besteht, stellt sich die Frage, ob die Maßnahme unter eine der bestehenden Normen gefasst werden kann. In Betracht zu ziehen sind hier insbesondere §§ 100 a ff. StPO.

1. §§ 100 a, 100 b StPO

Da sich die Ermittler bei der „stillen SMS" der Technik und Geräte der Telekommunikation bedienen, ist zunächst an die diesbezüglichen Rechtsgrundlagen zu denken. §§ 100 a, 100 b StPO regeln die Überwachung der Telekommunikation, worunter die Kenntnisnahme von Inhalt und Verbindungsdaten zu verstehen ist.[8] Erfasst sind hiervon auch die Standortdaten, so dass deren *Abfrage* zulässig sein soll (dazu unten 4.). Die „stille SMS" beinhaltet indes auch die *Erzeugung* dieser Daten, die also ebenfalls von § 100 a StPO abgedeckt sein müsste. Bei der Überwachung der Telekommunikation handelt es sich aber um eine grundsätzlich passive Tätigkeit; ein aktives Vorgehen ist nur insoweit zulässig, als es den für diese Kenntnisnahme notwendigen Zugang zu den betreffenden Daten schafft.[9] Das im Rahmen der Ermittlungsmethode der „stillen SMS" praktizierte „pingen" stellt sich jedoch als aktive Maßnahme dar, die nicht erst den Zugang zu, sondern die Schaffung von Daten betrifft. Es lässt sich daher nicht unter das Tatbestandsmerkmal „Überwachung der Telekommunikation" fassen und ist somit nicht vom Wortlaut gedeckt. Etwas anderes könnte nur gelten, wenn man als Telekommunikation bereits das bloße Bereitstellen einer Leitung für die Datenübertragung versteht. Dies steht jedoch nicht nur im Widerspruch zum Wortsinn, sondern auch zur Legaldefinition in § 3 TKG, die Telekommunikation auf das Aussenden, Übermitteln und Empfangen von Nachrichten beschränkt.

Für andere Überwachungsmaßnahmen, wie den Einsatz technischer Mittel nach § 100 c StPO, wird zwar teilweise vertreten, dass nicht ausdrücklich geregelte Eingriffe, die für die eigentliche Maßnahme notwendig und dieser vorgelagert sind, von den betreffenden Normen mit erfasst seien.[10] Gleichwohl lässt sich diese Konstruktion nicht auf den vorliegenden Sachverhalt übertragen, da es sich beim Aussenden des „ping" nicht um eine für die Überwachung nach § 100 a StPO notwendige Maßnahme handelt. Sie ermöglicht vielmehr eine weitergehende Überwachung, so dass die Voraussetzungen für die Annahme einer Annexkompetenz nicht gegeben sind. Angesichts des abschließenden Charakters der §§ 100 a, 100 b StPO und der Unzulässigkeit einer erweiternden Auslegung[11] können diese somit nicht als Rechtsgrundlage dienen.

2. §§ 100 g I, 100 h StPO

§ 100 g I StPO regelt die Auskunft über Telekommunikationsverbindungsdaten durch die Mobilfunkbetreiber. Hierunter fällt gemäß der Legaldefinition in Abs. 3 Nr. 1 auch die Standortkennung, also die Daten, die von den Ermittlern mit Hilfe der „stillen SMS" erzeugt werden. Gleichwohl erfasst die Vorschrift nach ihrem Wortlaut ebenfalls nur die Auskunft über die Daten, nicht jedoch ihre Erzeugung, wie durch die Formulierung „im Falle einer Verbindung" in Abs. 3 Nr. 1 unterstrichen wird.[12] Die Norm kann daher – zumindest alleine – ebenso wenig als Rechtsgrundlage für die „stille SMS" dienen.

3. § 100 i I Nr. 2 bzw. § 100 c I Nr. 1 b, II und III StPO i. V. m. §§ 100 a, 100 b bzw. §§ 100 g I, 100 h StPO

Da die genannten Rechtsgrundlagen jedenfalls nicht das aktive „pingen" erfassen, wurde von verschiedener Seite vorgeschlagen, die „stille SMS" auf mehrere Rechtsgrundlagen zu stützen.[13] Danach lasse sich die Maßnahme in einen lediglich Daten erzeugenden Schritt („ping") sowie die dann folgende Abfrage beim Mobilfunkanbieter aufteilen, die jeweils von verschiedenen Rechtsgrundlagen gedeckt seien. Für den ersten Schritt kommen dabei zunächst die Spezialermächtigungen der §§ 100 i I Nr. 2 und 100 c I Nr. 1 b, II und III StPO in Betracht, die jedoch beide nicht die Abfrage der erzeugten Daten durch Heranziehung der Mobilfunkanbieter ermöglichen.[14] Für diesen zweiten Schritt wären §§ 100 a, 100 b bzw. 100 g I, 100 h StPO als Rechtsgrundlage denkbar.

Unabhängig von der Zulässigkeit einer solchen Aufspaltung (dazu unten 5.) stellt sich hierbei bereits die Frage, ob die genannten Rechtsgrundlagen die beiden Schritte der „stillen SMS" decken.

a) § 100 i I Nr. 2 StPO als Rechtsgrundlage für das Aussenden des Signals

Vom Wortlaut her betrachtet scheint § 100 i I Nr. 2 StPO die „stille SMS" bzw. das Aussenden des Signals zunächst zu erfassen, auch wenn der Anwendungsbereich durch die engen Voraussetzungen erheblich eingeschränkt wäre. Tatsächlich aber ist die Norm bereits vom Wortlaut her alleine auf den IMSI-Catcher zugeschnitten. Nach Abs. 1 Nr. 2 darf *durch technische Mittel* der Standort eines Mobilfunkendgerätes ermittelt werden. Das einzige technische Mittel, das diese Funktion ohne weitere Schritte und Hilfsmittel erfüllt, ist indes der IMSI-Catcher. Bei dem „ping" handelt es sich demgegenüber um ein technisches Mittel, das erst in Kombination mit der Datenabfrage beim Mobilfunkanbieter eine Standortermittlung möglich macht, so dass es unmittelbar vom Wortlaut nicht erfasst ist.

Diese bereits durch den Wortlaut nahe gelegte Auslegung wird durch eine historische Betrachtung bestätigt. Der Gesetzesgeber hatte bei der Schaffung des § 100 i StPO einzig und alleine den IMSI-Catcher im Auge, für den aufgrund der besonderen Eingriffskonstellation eine eigene Norm gebildet wurde. Andere Maßnahmen sollten hierdurch nicht ermöglicht werden.[15] Systematisch ist zu beachten, dass Abs. 4 S. 4 zum einen davon spricht, dass für die von der Norm gemeinte Methode der Standortbestimmung die Geräte- und Kartennummer des Endgerä-

5) Vgl. BT-Dr 15/1448, S. 1 f.; LT-Dr 15/352 (Niedersachsen), S. 2; AbgH-Dr 15/10 559 (Berlin), S. 1. Dabei werden zum Erstellen von genauen und regelmäßigen Bewegungsbildern nicht selten mehrere hundert „stille SMS" pro Fall versandt. – Vgl. indes zur Unzulässigkeit optischer Ermittlungsmaßnahmen betreffend Wohnungen *Mitverf.* NStZ 2002, 638 ff.

6) Vgl. BT-Dr 15/1448, S. 2; LT-Dr 15/352 (Niedersachsen), S. 3; Presseerklärung des Berliner Innensenators vom 24. 10. 2003.

7) Umfassend hierzu *Gercke* Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, S. 41 ff.

8) *Mitverf.* BeweisR der StPO 4. Aufl., Rn 2402.

9) Vgl. *Meyer-Goßner* 46. Aufl., § 100 a Rn 3; s. auch KK-*Nack* 5. Aufl., § 100 a Rn 7 ff., 13 f. mit indes undeutlicher Bewertung der „stillen SMS".

10) *Meyer-Goßner* § 100 c Rn 8 mwN. S. auch *Mitverf.* (o. Fn 8), Rn 2427.

11) Vgl. *BGHSt* 31, 296, 298; 31, 304, 306.

12) Vgl. KK-*Nack* § 100 g Rn 9.

13) Vgl. BT-Dr 15/1448, S. 2 f.; LT-Dr 15/352 (Niedersachsen), S. 3 f.

14) *Gercke* (o. Fn 7), S. 110 ff.

15) Vgl. *Hilger* GA 2002, 557, 558 f.

tes erforderlich sind. Dies ist nur beim IMSI-Catcher der Fall, während für die "stille SMS" alleine die Rufnummer ausreicht. Zum anderen wird an dieser Stelle eine Auskunftspflicht der Mobilfunkbetreiber statuiert, die jedoch nicht die Datenabfrage im Rahmen der „stillen SMS" zulässt. Beides spricht dafür, dass das Merkmal „technische Mittel" in § 100 i StPO nur den IMSI-Catcher erfasst. Dies wird durch eine teleologische Betrachtung bestätigt. Sinn und Zweck des Abs. 1 Nr. 2 sind alleine die Ermittlung des aktuellen Standorts für einen Zugriff – Weitergehendes ist mit dem recht umständlichen IMSI-Catcher auch kaum möglich. Demgegenüber scheint die „stille SMS" in der Praxis vor allem bis ausschließlich für darüber hinausgehende und damit regelmäßig eingriffsintensivere Zwecke eingesetzt zu werden.[16]

All dies zusammengenommen zwingt dazu, § 100 i Abs. 1 Nr. 2 StPO so auszulegen, dass nur der IMSI-Catcher erfasst wird. Das Aussenden des „ping" bei der „stillen SMS" ist daher von der Norm nicht gedeckt.

b) § 100 c I Nr. 1 b, II und III StPO als Rechtsgrundlage für das Aussenden des Signals

Da die „stille SMS" in der Praxis offenbar häufig observationsunterstützend eingesetzt wird, kommt sodann § 100 c I Nr. 1 b, II und III StPO als spezielle Rechtsgrundlage in Betracht. Dafür müsste es sich bei der „stillen SMS" um ein sonstiges besonderes für Observationszwecke bestimmtes technisches Mittel handeln, was indes nicht zweifelsfrei ist. Der Gesetzgeber hatte bei der Schaffung der Norm vor allem Peilsender und vergleichbare Mittel im Auge, die eigentlich nur im Zusammenhang mit Observationen zum Einsatz kommen.[17] Gleichwohl lässt der nicht ganz genaue Wortlaut der Norm auch eine extensivere Auslegung zu, die insbesondere im Hinblick auf Sinn und Zweck der Vorschrift nicht völlig fern liegend zu sein scheint.[18] So wird z. B. das Global Positioning System, das in seinem Eingriffscharakter der „stillen SMS" ähnelt, nach wohl überwiegender Auffassung als von der Norm gedeckt angesehen. Wegen der besonderen Qualität des Eingriffs durch dieses und der im Vergleich zu § 100 a StPO vereinfachten Zuständigkeitsregelung ist dabei aber ohnehin eine Beschränkung auf Ausnahmefälle oder eine entsprechende Anwendung der Subsidiaritätsklausel des Abs. 1 Nr. 2 angezeigt.[19] Mindestens dies müsste demnach auch für die „stille SMS" gelten, wenn man das Aussenden des Signals als von § 100 c I Nr. 1 b gedeckt ansehen wollte.

Weiterhin ist aber zu berücksichtigen, dass hier die gleichen systematischen Bedenken wie bei § 100 i StPO bestehen – denn die Norm regelt ebenso wenig die notwendige Auskunftspflicht der Mobilfunkbetreiber –, so dass teilweise vertreten wird, die Ortung mit Hilfe von Mobilfunkendgeräten richte sich ausschließlich nach § 100 a StPO.[20]

c) Fazit

Somit kann weder § 100 c I Nr. 1 b StPO noch § 100 i Abs. 1 Nr. 2 StPO grundsätzlich das Aussenden des Signals decken, weshalb eine Kombination dieser Normen mit §§ 100 a, 100 b bzw. §§ 100 g Abs. 1, 100 h StPO keine hinreichende Rechtsgrundlage für die Ermittlungsmethode der „stillen SMS" bietet.

4. §§ 163 I, 161 I StPO i. V. m. §§ 100 a, 100 b bzw. 100 g I, 100 h StPO

Denkbar wäre jedoch, dass die Generalklauseln §§ 163 I, 161 I StPO das Aussenden des Signals erfassen, so dass diese in Kombination mit den §§ 100 a, 100 b bzw. §§ 100 g I, 100 h StPO eine Rechtsgrundlage für die „stille SMS" liefern könnten.[21]

a) §§ 163 I, 161 I StPO als Rechtsgrundlage für das Aussenden des Signals

aa) Beide Normen fungieren seit dem Strafverfahrensänderungsgesetz 1999 als Ermittlungsgeneralklauseln und bilden so die Rechtsgrundlage für einfache Maßnahmen von Polizei und StA.[22] Damit hat sich zwar der Streit um die Qualität der Regelungen und die Frage der Legitimation für derartige Eingriffe erledigt. Aktuell bleibt jedoch die Frage, für welche Maßnahmen die Generalklauseln ausreichend sind und wann eine spezielle Ermächtigung nötig wird.[23] Dabei ist einerseits zu berücksichtigen, dass nicht jede Ermittlungsmaßnahme spezialgesetzlich erfasst werden kann. Andererseits erfordert der verfassungsrechtliche Bestimmtheitsgrundsatz, dass gesetzliche Ermächtigungen zu Grundrechtseingriffen nach Art und Umfang hinreichend bestimmt sind, so dass der mögliche Eingriff für den Bürger berechenbar wird. Dies gilt umso mehr, je intensiver der Eingriff ist.[24] Mithin können die durchaus weit gefassten §§ 163 I, 161 I StPO nur für niedrigschwellige Grundrechtsbeeinträchtigungen herhalten.[25] Als Abgrenzungskriterien hierfür wurde vorgeschlagen, ob die Ermittlungsmaßnahme mit Zwang verbunden ist, heimlich vorgenommen wird oder der Erhebung privater, vor staatlichem Zugriff geschützter Daten dient.[26]

Das Erzeugen von Daten beim Mobilfunkbetreiber mittels „ping" wäre somit von den Generalklauseln nur gedeckt, wenn es kein oder nur ein niedrigschwelliger Grundrechtseingriff wäre. In Betracht kommt hier neben Art. 10 GG vor allem eine Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG[27], das die Befugnis des Einzelnen beinhaltet, selbst zu entscheiden, ob und wie persönliche Lebenssachverhalte offenbart werden.[28] Hierzu gehört auch die Information, wo sich eine Person zu einem bestimmten Zeitpunkt aufhält. Ein Eingriff in das Grundrecht ist gegeben, wenn solche Daten erhoben, gespeichert, verwendet oder weitergegeben werden. Die Grenzen dessen sind im Einzelnen unklar, aber jedenfalls überschritten, wenn der Staat sich die Information verschafft, zu welchem Zeitpunkt sich eine bestimmte Person wo aufhält.[29] Fraglich ist lediglich, *ob* ein solcher *Eingriff* erst

16) S. oben I.2.

17) BT-Dr 12/989, S. 39.

18) Vgl. hierzu *BGHSt* 46, 266, 271 f. Für eine restriktive Auslegung *Comes* StV 1998, 569, 569 f.

19) *Mitverf.* (o. Fn 8), Rn 2427 mwN.

20) KK-*Nack* § 100 c Rn 9, 12.

21) So auch die Bundes- und einige Landesregierungen in ihren diesbezüglichen Stellungnahmen; BT-Dr 15/1448, S. 2 f.; LT-Dr 15/352 (Niedersachsen), S. 3 f. Die Bundesregierung geht dabei davon aus, dass über § 100 g StPO nur eine einzelfallbezogene Auskunftserteilung möglich ist, während die Abfrage von Bewegungsbildern § 100 a StPO unterfalle.

22) *Hilger* NStZ 2001, 561, 563 f.; *Meyer-Goßner* § 161 Rn 1, § 163 Rn 1, 28 ff.

23) Wenig ergiebig ist dabei die Aufteilung in „tiefer" und „weniger tief" in Grundrechte eingreifende Maßnahmen, wie sie sich auch in der Gesetzesbegründung findet, vgl. KK-*Nack* § 161 Rn 1.

24) *Di Fabio* in *Maunz/Dürig* 40. Lfg., Art. 2 I Rn 182 ff.

25) *Gercke* (o. Fn 7), S. 115 f. mwN.

26) *Hefendehl* StV 2001, 700, 703 f. mwN; s. auch *Hilger* NStZ 2001, 561, 564.

27) Zwar ist das Fernmeldegeheimnis im Verhältnis zu Art. 2 I i. V. m. Art. 1 I GG grundsätzlich spezieller. Im Rahmen der vorliegenden Konstellation liegt der Schwerpunkt des Eingriffs jedoch nicht bei der von Art. 10 GG geschützten Kommunikation, sondern bei der Standortbestimmung (vgl. zu dieser Abgrenzung unten c.), so dass spätestens bei der in der Praxis offenbar vor allem relevanten intensiveren Überwachung zur Bewegungsbilderstellung von einem Vorrang von Art. 2 I i. V. m. Art. 1 I GG auszugehen ist (so auch KK-*Nack* § 100 a Rn 14).

28) *BVerfGE* 65, 1, 41 ff.; *Dreier* GG, Art. 2 I Rn 52.

29) Vgl. *Dreier* (o. Fn 27); *Di Fabio* (o. Fn 24), Rn 176.

gegeben ist, wenn den Ermittlern die Daten vom Mobilfunkbetreiber übermittelt werden oder ob nicht *bereits die Erzeugung der* dann abzufragenden *Daten* als Eingriff bzw. dessen Beginn angesehen werden muss.

bb) Ersterer Auffassung ist zunächst zuzugestehen, dass eine Aufspaltung der Maßnahme in einen Daten erzeugenden und einen abfragenden Schritt rein denklogisch möglich ist. Danach scheint eine grundrechtliche Beeinträchtigung erst dann gegeben zu sein, wenn die Ermittler die Daten erhalten, das heißt beim Mobilfunkbetreiber abfragen. Indes mutet diese Betrachtungsweise eher gekünstelt an, denn realiter folgen das Senden des Signals und die Übermittlung der Daten unmittelbar aufeinander, so dass sich die beiden Schritte schon bei tatsächlicher Betrachtung kaum trennen lassen und vielmehr als einheitlicher Vorgang der Datenerhebung anzusehen sind.

Sinn und Zweck des Grundrechts auf informationelle Selbstbestimmung ist unter anderem, den für eine individuelle Selbstbestimmung notwendigen Freiraum zu schützen, in dem man davon ausgehen kann, dass das eigene Verhalten nicht erfasst und gespeichert wird, so dass kein Konformitätsdruck entsteht.[30] Dieser Schutzweck ist jedoch bereits empfindlich tangiert, wenn staatliche Stellen eine Speicherung von Daten veranlassen und die bloße *Möglichkeit* besteht, dass sie hiervon auch Kenntnis erlangen. Demnach wäre schon die Veranlassung der – nur beim Mobilfunkanbieter erfolgenden – Speicherung der Daten durch den „ping" als Eingriff zu werten, zumal die Übermittlung der Daten an die Ermittler in aller Regel tatsächlich erfolgt. Dem ließe sich zwar entgegenhalten, dass diese Übermittlung – wenn überhaupt – nur unter den engen Voraussetzungen von § 100 a bzw. § 100 g StPO zulässig ist. Dies enthebt den Betroffenen jedoch nicht von seinen Befürchtungen und dem damit verbundenen Konformitätsdruck, insbesondere da mit der Möglichkeit der Bewegungsbilderstellung eine überaus intensive Beeinträchtigung der informationellen Selbstbestimmung droht. Zudem ist anerkannt, dass die staatliche Weitergabe von Daten an Dritte einen selbständigen Eingriff in das informationelle Selbstbestimmungsrecht darstellt.[31] Es ist aber nicht einzusehen, warum dies anders sein sollte, wenn dem Dritten die Daten nicht durch Weitergabe, sondern auf anderem Wege zugänglich gemacht werden. Der geschützte Freiraum ist also schon mit der Erzeugung und Speicherung der Daten beeinträchtigt und ein Eingriff daher bereits anzunehmen – anderenfalls wäre die Speicherung von Bewegungsbildern aller einer Straftat Verdächtigen bei den Mobilfunkanbietern zulässig.

Hierfür spricht auch, dass es sich bei der Erzeugung der Daten durch das *Aussenden des Signals* keineswegs um eine bloße Vorstufe der eigentlichen Maßnahme handelt. Vielmehr stellt sie *deren Kern* und ihre Besonderheit dar, da nur so die exakte Standortbestimmung zu jedem beliebigen Zeitpunkt und das Abfragen eines genauen Bewegungsprofils möglich wird. Dies führt zu folgender Überlegung: Würde man die Datenerzeugung nicht oder nur als geringfügigen Eingriff werten und damit als von §§ 163 I, 161 I StPO gedeckt ansehen, so würde durch die Aufteilung der Maßnahme auf verschiedene Rechtsgrundlagen letztlich ein weitergehender Grundrechtseingriff zulässig, als von §§ 100 a, 100 g StPO alleine gedeckt wäre. Die Generalklauseln würden also mittelbar – durch die Kombination mit §§ 100 a, 100 g StPO – einen Grundrechtseingriff ermöglichen, der von speziellen Ermächtigungen alleine nicht erfasst wäre, obwohl sie hierfür gerade nicht ausreichend sind. Dies widerspräche der Systematik der StPO, wonach spezielle Maßnahmen einer speziellen Rechtsgrundlage bedürfen.

cc) Ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung liegt bei der "stillen SMS" somit bereits beim Aussenden des Signals vor. Dieser erfolgt auch heimlich und unter Einwirkung auf die Privatsphäre. Dass der Betroffene die Einwirkung durch den Betrieb und das Mitführen des Handys erst ermöglicht, ändert an dieser Bewertung nichts, denn er macht seine Standortdaten damit nicht frei zugänglich. Diese sind vielmehr vor dem Zugriff Dritter geschützt.[32] Das Aussenden des Signals stellt mithin einen nicht nur leichten Grundrechtseingriff dar und ist deshalb nicht mehr von §§ 163 I, 161 I StPO gedeckt.[33]

b) §§ 100 g I, 100 h StPO als Rechtsgrundlage für die Abfrage der erzeugten Daten

Selbst wenn dem nicht gefolgt würde, scheint darüber hinaus fraglich, ob spezielle Eingriffsgrundlagen die Abfrage der erzeugten Daten und damit den zweiten Schritt der „stillen SMS" zulassen. Hierfür kommt zunächst § 100 g StPO in Betracht, dessen Reichweite bezüglich der Standortkennung aufgrund der Einschränkung „im Falle einer Verbindung" in der Legaldefinition des Abs. 3 Nr. 1 umstritten ist.[34] Davon nicht erfasst sind jedenfalls die im stand by-Betrieb anfallenden Daten – ansonsten wäre die Einschränkung überflüssig. Auch hatte der Gesetzgeber die Aufnahme einer derart umfassenden Auskunftspflicht und Überwachungsmöglichkeit ausdrücklich abgelehnt. Fraglich bleibt aber, ob das Aussenden des „ping"-Signals als Verbindung im Sinne der Legaldefinition angesehen werden kann. Hierfür spricht, dass im Gegensatz zum stand by-Betrieb eine aktive Kommunikation zwischen den beteiligten Endgeräten und dem Funknetz stattfindet, die man zumindest vom Wortsinn her als Verbindung qualifizieren könnte.

Andererseits wäre damit die Absicht des Gesetzgebers ad absurdum geführt, eine Abfrage der stand by-Daten nicht zuzulassen. Denn die Ermittler müssten zwar vorher das Signal aussenden, hätten bei der Abfrage aber ein vergleichbares Ergebnis: Standortdaten auch ohne dass der Betroffene sein Endgerät benutzt. Besonders problematisch hieran ist, dass so die Erstellung exakter Bewegungsbilder möglich wird, die ansonsten höchstens unter den engeren Voraussetzungen des § 100 a StPO möglich wäre. Vor diesem Hintergrund muss der Terminus „Verbindung" in Abs. 3 Nr. 1 enger ausgelegt werden, so dass die Abfrage der mit dem „ping" erzeugten Standortdaten auf der Grundlage des § 100 g I StPO ausgeschlossen ist.[35]

c) §§ 100 a, 100 b StPO als Rechtsgrundlage für die Abfrage der erzeugten Daten

Schließlich kommen als Rechtsgrundlage für das Abfragen der Daten bei den Mobilfunkbetreibern die Regelungen zur Überwachung der Telekommunikation in Be-

30) *BVerfGE* 65, 1, 42 ff.; *Di Fabio* (o. Fn 24), Rn 175.

31) Vgl. *Di Fabio* (o. Fn 24), Rn 176.

32) Vgl. *Hefendehl* StV 2001, 700, 703 f. mwN. Insoweit weicht der Sachverhalt von der diesbezüglich ohnehin nicht unbedenklichen Entscheidung *BGHSt* 42, 139, 154 ab.

33) Nichts anderes ergibt sich aus dem Vergleich mit der Konstellation des ebenfalls nicht ganz unproblematischen sog. „Kontrollanrufs" für die Erzeugung sodann abzufragender Daten (vgl. *LG Aachen* m. abl. Anm. *Bernsmann/Jansen* StV 1999, 590, 591 f.; *Artkämper* Kriminalistik 1998, 202, 206). Zum einen ist diese einmalige Standortfeststellung wesentlich weniger eingriffsintensiv als die in der Praxis der „stillen SMS" regelmäßig wiederholt erfolgende Ortung bis hin zum Bewegungsbild. Andererseits handelt es sich um eine nicht gänzlich heimliche Maßnahme, auch wenn der Betroffene den dahinter stehenden Zweck nicht erkennen mag.

34) Dazu umfassend *Demko* NStZ 2004, 57, 58 f.

35) Ebenso KK-*Nack* § 100 g Rn 9 f.

tracht. § 100a StPO erfasst neben den Inhalts- auch die Verbindungsdaten und damit auch die Standortkennung – jedenfalls solange sie anlässlich aktiver Kommunikation anfällt. Auch an dieser Stelle erweist sich aber die Betrachtung der Rechtslage für die Abfrage bloßer stand by-Daten als fruchtbar, da die Ergebnisse der Maßnahmen und damit auch die Problemlagen vergleichbar sind.

Ob § 100a StPO den Abruf von stand by-Daten zulässt, ist in höchstem Maße umstritten. Die Rechtsprechung und Teile der Literatur bejahen dies unter extensiver Auslegung des Begriffs Telekommunikation.[36] Indes scheint es bereits problematisch, das reine Mitführen eines eingeschalteten Handys als Kommunikation zu bezeichnen, auch wenn das Gerät in gewissen Abständen Signale an das Funknetz abgibt, und auch systematisch und teleologisch ist dieses Vorgehen wenig stimmig. Die Normen der Telekommunikationsüberwachung sollen den Ermittlungsbehörden die Kenntnisnahme von Inhalt und Begleitumständen aktiver verbaler Kommunikation ermöglichen. Im Gegensatz dazu geht es bei der Ortung und Erstellung von Bewegungsbildern mit Hilfe von Mobilfunkgeräten sachlich gar nicht mehr um Kommunikation. Vielmehr bedienen sich die Ermittler lediglich der *als Peilsender fungierenden Technik* für Maßnahmen, die vor allem dem Bereich der Observation zuzuordnen sind und denen eine grundsätzlich andere Eingriffsrichtung im Hinblick auf Grundrechte innewohnt.[37] Demnach kann die Abfrage von stand by-Daten nicht auf § 100a StPO gestützt werden.

Hinsichtlich der mit „stiller SMS" erzeugten Daten ist zwar zu konstatieren, dass diese auch unter einen engeren Telekommunikations-Begriff gefasst werden können. Systematisch und teleologisch bestehen jedoch die gleichen Bedenken, wie bei dem Abruf von stand by-Daten. Zudem würde die Zulässigkeit der „stillen SMS" im Ergebnis dazu führen, dass die Unzulässigkeit der Abfrage von stand by-Daten umgangen würde.

d) Fazit

Zusammenfassend lässt sich daher feststellen, dass die StPO weder für das Aussenden des Signals noch die Abfrage der so erzeugten Daten im Rahmen der „stillen SMS" eine Rechtsgrundlage bereitstellt. Mithin ist auch eine Kombination aus §§ 163 I, 161 I i. V. m. §§ 100a, 100b bzw. §§ 100g I, 100h StPO keine hinreichende Rechtsgrundlage für diese Ermittlungsmethode, so dass diese de lege lata nicht von den Eingriffsnormen der StPO gedeckt und damit rechtswidrig ist.

5. Zur grundsätzlichen Unzulässigkeit der Aufspaltung von Maßnahmen

Ungeachtet der ausgeführten Bedenken hinsichtlich der Anwendung der einzelnen Normen auf die „stille SMS" stellt sich allgemein die Frage, ob die Konstruktion der Aufspaltung und Aufteilung einer Maßnahme auf verschiedene Rechtsgrundlagen als zulässig angesehen werden kann. Dies gilt vorliegend insbesondere vor dem Hintergrund, dass bei einer Aufspaltung der Maßnahme die genaue Bestimmung des Eingriffs schwerlich möglich ist (zu den in diesem Zusammenhang genannten Argumenten s. oben 3.).

a) Ausgangspunkt einer solchen Betrachtung müssen die Grundrechte und der mit den Ermittlungsmaßnahmen verbundene Eingriff in diese sein. Neben dem Post- und Fernmeldegeheimnis aus Art. 10 GG ist bei den in Rede stehenden Maßnahmen regelmäßig auch das Allgemeine Persönlichkeitsrecht aus Art. 2 I i. V. m. Art. 1 I GG bzw. das Grundrecht auf informationelle Selbstbestimmung als Bestandteil dessen tangiert. Eingriffe in diese lassen sich nur aufgrund hinreichend spezieller und bestimmter Ermächtigungen rechtfertigen, insbesondere muss für den Bürger erkennbar sein, welche Maßnahmen mit diesen Eingriffsgrundlagen möglich sind.[38] Demgegenüber würde die Aufspaltung von Ermittlungsmaßnahmen und ihre Stützung auf verschiedene Rechtsgrundlagen zu einer gegenläufigen Auswirkung führen. Einerseits würde auf diesem Wege ein Mehr an Eingriffen legitimiert, das vom Gesetzgeber regelmäßig gerade nicht vorgesehen war, und es würde so das Erfordernis einer spezialgesetzlichen Grundlage indirekt umgangen und ausgehöhlt. Zum anderen wäre für den Bürger angesichts der ohnehin zahllosen, unübersichtlich geregelten Eingriffsgrundlagen kaum mehr voraussehbar, welche Eingriffe in sein Grundrecht möglich sind und welche nicht, wenn die Normen beliebig kombiniert werden könnten. Schließlich würde damit der ohnehin bestehenden Tendenz Vorschub geleistet, unter Vernachlässigung einer Prüfung der Rechtslage für Ermittlungszwecke verschiedene Maßnahmen einzusetzen, die technisch möglich sind (dazu unten III.). Dies gilt umso mehr, da die in Rede stehenden Eingriffe nicht selten verschiedene Grundrechte sowie den gesamten Lebensbereich betreffen – z. B. wenn es um die Erstellung von Bewegungsbildern geht – und somit von erheblicher Intensität sind. Denn daraus folgt nicht nur ein besonderes Gewicht des Grundsatzes der Verhältnismäßigkeit.[39] Vielmehr sind auch an die Bestimmtheit der Eingriffsnormen erhöhte Anforderungen zu stellen, und es ist eine restriktive Auslegung dieser als abschließend angezeigt. Für Eingriffe, die über die in den einzelnen Normen jeweils geregelten Maßnahmen hinaus gehen, ist deshalb grundsätzlich eine eigene, hinreichend bestimmte Rechtsgrundlage notwendig.

Über diese grundrechtsdogmatische Betrachtung hinaus werden einer Aufteilung auf mehrere Rechtsgrundlagen im Rahmen der Auslegung regelmäßig systematische, historische und ggf. auch teleologische Argumente entgegenstehen, nachdem der Gesetzgeber die Maßnahme nicht vollständig in einer Norm geregelt hat, so dass eine Aufspaltung auch hiernach unzulässig ist.

b) Ausnahmen von diesen Grundsätzen könnten höchstens für klar aufteilbare Ermittlungsmethoden erwogen werden, deren nicht durch die ansonsten einschlägige spezielle Rechtsgrundlage geregelter Teil keinen Schwerpunkt der Maßnahme bildet und zudem keinen oder nur einen sehr leichten Grundrechtseingriff darstellt, so dass er als beiläufiger Bestandteil angesehen werden kann.[40] All dies trifft auf die „stille SMS" nicht zu. Die Maßnahme lässt sich zum einen kaum aufteilen. Zum anderen bildet das Aussenden des Signals keinen bloß beiläufigen Bestandteil, sondern ist vielmehr mindestens ein Schwerpunkt der Ermittlungsmethode, der ihr erst den über die anderen

36) *BGH* [ER] StV 2001, 214, 215 f. mwN; *Artkämper* Kriminalistik 1998, 202, 206; KK-*Nack* § 100a Rn 14, 20.

37) *Bernsmann* NStZ 2002, 103, 103 f.; *Deckers* StraFo 2002, 109, 112; *Gercke* (o. Fn 7), S. 92 ff. Detailliert hierzu *Demko* NStZ 2004, 57, 60 ff. mwN, die daher und im Anschluss an die Differenzierung zwischen Daten und daraus zu entnehmenden Informationen de lege feranda für eine Trennung und besondere Regelung im Bereich der Normen zur Observation eintritt.

38) *BVerfGE* 65, 1, 42 ff.

39) KK-*Nack* § 100a Rn 14 mwN.

40) Für zwingend mit der geregelten Maßnahme verbundene weitere, leichte Eingriffe wird teilweise eine Annexkompetenz angenommen, vgl. *Meyer-Goßner* § 100c Rn 8 mwN. Bei Maßnahmen wie der „stillen SMS" handelt es sich jedoch nicht um eine solche Konstellation, siehe hierzu bereits oben 1. Ebenfalls anders verhält es sich, wenn zwei grundsätzlich selbständige Eingriffe aufeinander folgen und nur mittelbar zusammenhängen, wie z. B. die Durchsuchung mit anschließender Beschlagnahme. Denn das Aussenden des „ping" ist mit der folgenden Abfrage der Daten immer und notwendig verbunden; es würde alleine keinen Sinn ergeben.

Ermittlungsmöglichkeiten hinausgehenden Sinn verleiht und auch bereits einen Grundrechtseingriff bedeutet (vgl. oben 3.).

6. Fazit

Die heimliche Ortung per „stiller SMS" ist somit nicht durch die bestehenden Eingriffsgrundlagen gedeckt und daher rechtswidrig. Dies gilt sowohl für die einmalige Anwendung zur Feststellung des Aufenthaltsortes, als auch für die wiederholte Ortung zur Unterstützung von Observationen, Erstellung von Bewegungsbildern etc. Insbesondere lässt sich die Maßnahme nicht aufteilen und auf mehrere Rechtsgrundlagen stützen. Dies ist vielmehr auch allgemein grundsätzlich unzulässig.

III. Zur Problematik der Ausweitung von Eingriffsgrundlagen durch die Praxis und der zunehmenden Möglichkeiten heimlicher Überwachung

Die rechtlich unzulässige Verwendung der „stillen SMS" ist ein erneutes Beispiel dafür, dass sich die Praxis der Ermittlungsbehörden weniger an den geschaffenen Eingriffsgrundlagen als mehr am *Stand der Technik* orientiert. Was technisch möglich ist, *wird* auch *eingesetzt*.[41] Dies erscheint besonders problematisch, da solche Maßnahmen vor allem im verdeckten Bereich eingesetzt und von den Behörden geheim gehalten bzw. wenn überhaupt regelmäßig erst im Rahmen der Hauptverhandlung bekannt werden, so dass sie ggf. der öffentlichen Diskussion wie auch dem Rechtsschutz des Betroffenen (vorerst) entzogen sind.[42] Die Präventivkontrolle durch den teilweise bestehenden Richtervorbehalt kann dies nur wenig mildern, da hier nur aufgrund einer einseitigen Tatsachengrundlage und in der Praxis nicht selten durch bloße Übernahme der Begründung der StA entschieden wird.[43]

Gleichzeitig werden mit diesem Vorgehen Tatsachen geschaffen, an denen die Rechtsprechung sich schwer tut, vorbeizukommen,[44] und die einen erheblichen Druck auf den Gesetzgeber bedeuten, der sich nicht dem Vorwurf ausgesetzt sehen mag, einer effektiven Strafverfolgung im Weg zu stehen.[45] Auf diesem Weg entsteht gleichsam ein *Automatismus* der Schaffung von Rechtsgrundlagen, dessen Tempo im wesentlichen von der Exekutive bestimmt wird, und der zu immer weitergehenden Möglichkeiten der Überwachung führt.[46] Diese Entwicklung wird dadurch verstärkt, dass der technische Fortschritt praktisch ständig neue, effektivere und einfachere Überwachungsmethoden ermöglicht,[47] was zum einen bei den Ermittlern Ressourcen freimacht für weitere Ermittlungen. Vor allem aber bedeuten diese Maßnahmen – wie das Beispiel der Bewegungsbilderstellung zeigt – zunehmend intensivere Eingriffe in die einschlägigen Grundrechte, allen voran in das Grundrecht auf informationelle Selbstbestimmung.[48] Hand in Hand mit den verschiedensten, in den verdachtsunabhängigen Bereich des Polizeirechts vorverlagerten Eingriffsbefugnissen[49] haben diese *Möglichkeiten* zur Erforschung der Privat- und Intimsphäre zwischenzeitlich ein nur noch eingeschränkt kontrollierbares Ausmaß angenommen.

Diese Entwicklung führt, zusammen mit der Vorverlagerung in den präventiven, verdachtsunabhängigen Bereich, im Übrigen zu einer größer werdenden *(Selektions-)Macht* der *Polizei*. Im Zuge dessen entspricht es empirischer Erkenntnis, dass institutionalisierte Handlungsnormen[50] zu einer verstärkten Wirkung gelangen, so dass der durch die Zunahme von (heimlicher) Überwachung entstehende Konformitätsdruck sich z. B. nicht nur in Form der vorauseilenden Anpassung an herrschende Erwartungen vollzieht. Er findet vielmehr auch seine konkrete und erfahrbare Umsetzung, wenn die Beamten im Rahmen ihrer gesteigerten (Selektions-)Macht bei der Wahrnehmung und Verfolgung von Verdachtsmomenten im Sinne bestimmter Erscheinungsformen der Unangepasstheit der Betroffenen beeinflusst werden.[51] Insofern könnte die Strafverfolgung (mittelbar) eine durch die dargelegte Entwicklung verstärkte Durchsetzung von Anpassung bewirken, die mit dem ultima ratio-Gebot nichts mehr gemein hat.

41) Ebenso *Deckers* StraFo 2002, 109, 109 f., der aus der Praxis berichtet, dass eine Begrenzung der Eingriffe im Wesentlichen nur durch mangelnde Kapazitäten erfolge, so dass eine Steuerung (nur) über die Mittelzuteilung möglich wäre.

42) S. auch *Thommes* StV 1997, 657, 665.

43) Vgl. *Roxin* StrafverfahrensR 25. Aufl., S. 237 ff.

44) So auch *Hefendehl* StV 2001, 700, 702 mwN, der die gesamte Entwicklung dadurch verschärft sieht, dass § 163 StPO nun als Generalklausel fungiert.

45) Vergleichbares gilt, wenn die Exekutive (im Bereich der Prävention) Maßnahmen „nur" testet – wie im Falle des automatischen Kennzeichen-Abgleichs –, selbst wenn ein solcher Test durch Normen gedeckt sein sollte. Von der Struktur her ähnlich ist auch die Konstellation, dass eine eingriffsintensive Maßnahme zunächst eingeschränkt und unter sehr engen Voraussetzungen eingeführt wird, infolge des sicherheits- und kriminalpolitischen Diskurses aber eine immer weiter gehende Ausweitung erfährt, nachdem sie schon einmal eingeführt und die technischen Voraussetzungen für ihren Einsatz geschaffen wurden.

46) Verschärft wird diese Entwicklung durch die immer weiter gehende Schaffung von Befugnissen für präventive – mittlerweile gar alles erfassende – Eingriffe im Polizei- und Ordnungsrecht durch manche Länder, die einerseits eine frühzeitigere Überwachung ermöglichen und in deren Logik jeder Mensch zum potentiellen Risiko wird, aber gleichzeitig auch auf einen Ausbau der strafprozessualen Eingriffsbefugnisse drängen.

47) Bedeutsam in diesem Zusammenhang sind bspw. die Einführung von UMTS im Mobilfunk sowie die Technik der Radio-Frequency Identification (RFID); vgl. *Dix* Kriminalistik 2004, 81, 82 f.

48) Dies ist umso bedenklicher, als den Handelnden der Exekutive dieser Umstand nicht selten kaum bewusst zu sein scheint. So teilte bspw. der Berliner Innensenator in einer Presseerklärung vom 24. 10. 2003 zur „stillen SMS" mit: „Durch die bloße Ermittlung des Standortes wird der einzelne Bürger in seiner Privatsphäre praktisch überhaupt nicht beeinträchtigt."

49) Zur präventiven TKÜ *Dix* Kriminalistik 2004, 81, 84.

50) Hierzu umfassend *Mitverf.* Kriminologie 5. Aufl., § 40; speziell zu solchen bei den Staatsanwaltschaften *Singelnstein* MschrKrim 2003, 1 ff.

51) Betr. Verfolgungsintensität und jeweilige Beweiswürdigung etwa bereits *Endruweit* ZStW 85 (1973), 844 ff.; vgl. auch Beiträge in *Frehsee* u. a. (Hrsg.) Strafrecht, soziale Kontrolle, soziale Disziplinierung, Opladen 1993.

Professor Dr. Werner Beulke/Dr. Sabine Swoboda, Universität Passau

Trennscheibenanordnung „zum Schutz" des Strafverteidigers bei Verteidigerbesuchen im Strafvollzug?

– Besprechung des Beschlusses des BGH vom 3. 2. 2004 – 5 ARs (Vollz) 78/03 (OLG Karlsruhe)[1] –

I. Die Entscheidung

Der 5. *Senat* hatte über folgenden Sachverhalt zu befinden: Der Beschwerdeführer verbüßt eine langjährige Freiheitsstrafe mit anschließender Sicherungsverwahrung. In der Justizvollzugsanstalt kündigte der Beschwerdeführer an, Juristen und anstaltsfremde Personen töten zu wollen. Mit einem Schreiben an den Ministerpräsident des Landes

1) NJW 2004, 1398.