Strafprozessuale Maßnahmen bei Mobilfunkendgeräten

Die Befugnis zum Einsatz des sog. IMSI-Catchers

Von Stefanie Harnisch und Martin Pohlmann, Leipzig *

I. Einführung

"Reden Sie nicht so laut vom Datenschutz; Sie machen sich verdächtig. Beharren Sie nicht so stur auf Ihrer Privatsphäre; Sie werden sonst als Außenseiter registriert. (Aber registriert und kontrolliert werden Sie natürlich ohnehin.) Man meint es gut mit Ihnen, wenn man Ihr Telefon abhört, Ihre Verbindungen speichert und Ihre Computer durchsucht." [1]

In kaum einem anderen Bereich unserer Rechtsordnung ist der Hunger des Staates nach Daten so groß wie in dem der Strafverhinderung und -verfolgung. Durch immer neue Eingriffsbefugnisse und Ausweitungen bereits bestehender Regelungen dringt er in die Privatsphäre des Menschen ein und schafft zunehmend den von Datenschützern befürchteten "gläsernen Bürger". Besondere Relevanz kommt diesem Thema im Bereich der Telekommunikationsüberwachung zu, etwa aktuell bei der Problematik der Vorratsdatenspeicherung.[2] Nachdem es innerhalb der letzten zwanzig Jahre zu rasanten Entwicklungen auf dem Gebiet der Telekommunikationstechnik gekommen ist, hat sich für die organisierte Kriminalität ein neuer, da schwer zu überwachender Wirkbereich erschlossen. Ständige technische Neuentwicklungen zwingen den Staat zu immer weiter reichenden Regelungen, um eine effektive Strafverfolgung noch gewährleisten zu können. So wurde im Jahre 2002 der repressive Einsatz des IMSI-Catchers, eines technischen Hilfsmittels zur Überwachung der Telekommunikation, auf eine rechtliche Grundlage, § 100i StPO,[3] gestellt. Allerdings wurde das Gerät auch schon vor diesem Zeitpunkt eingesetzt.[4]

Der Einsatz des IMSI-Catchers ist jedoch rechtspolitisch durchaus umstritten. Einen Schwerpunkt des vorliegenden Beitrags bildet daher die kritische verfassungsrechtliche Würdigung der gesetzlichen Regelung in § 100i StPO. Dabei wird insbesondere deren Vereinbarkeit mit Art. 10 GG sowie Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu untersuchen sein. Entstehungsgeschichte und Novellierungen der Regelung sollen jedoch ebenso erörtert werden, wie deren praktische Bedeutung. Besonderes Augenmerk wird darüber hinaus auf die strafprozessualen Einsatzvoraussetzungen zu legen sein.

II. Grundlagen des IMSI-Catchers

Im Folgenden soll ein Überblick über die technischen und rechtlichen Grundlagen des Einsatzes des IMSI-Catchers[5] vermittelt werden.

1. Technische Grundlagen

a) Begriffsbestimmungen

aa) IMSI (Kartennummer)

Bei einer IMSI (International Mobile Subscriber Identity) handelt es sich um eine weltweit nur einmal vergebene Kennnummer, welche in GSM-Mobilfunknetzen einem jeden Teilnehmer (Vertragspartner eines Netzbetreibers) zugeordnet wird.[6] Sie ist auf einer speziellen, austauschbaren und in das Mobilfunktelefon eingelegten Chipkarte (SIM – Subscriber Identity Module) gespeichert,[7] welche jedem Teilnehmer mit Abschluss eines Mobilfunkvertrags

ausgehändigt wird.[8] Aufgrund ihrer Einmaligkeit vermag die IMSI-Nummer einen Mobilfunkteilnehmer weltweit in allen GSM-Netzen zu identifizieren.[9] Sie besteht aus einer fünfzehnstelligen Zahlenfolge, von denen die ersten fünf Ziffern Ländercode und Netzbetreiber erkennen lassen.[10] Anhand der weiteren Zeichen können die über den Netzbetreiber gespeicherten und ausschließlich ihm bekannten Bestandsdaten des Teilnehmers wie Mobilfunk-Rufnummer und Identität ermittelt werden.[11]

bb) IMEI (Gerätenummer)

Die IMEI (International Mobile Equipment Identity/elektronische Gerätekennung) ist ebenfalls eine international einmalig vergebene Kennnummer, welche mit einem Mobilfunkgerät (Handy) elektronisch verbunden ist.[12] Sie besteht ebenso wie die IMSI aus einer fünfzehnstelligen Ziffernfolge.[13]

cc) Funkzelle

Jedes Mobilfunknetz ist in sog. Funkzellen unterteilt, die den kleinsten Baustein des Netzes darstellen und eine bestimmte

geographische Fläche abdecken.[14] Die Größe einer Funkzelle bestimmt sich nach dem Bereich, welcher durch ihre Basisstation, den sog. Sendemast, der sich in der Mitte der Zelle befindet, abgedeckt wird. Die Zellen können je nach Wohndichte einen Radius von einigen hundert Metern bis hin zu mehreren Kilometern erreichen.[15]

b) Bedeutung der Kennungen (IMSI/IMEI)

Die Karten- und Gerätekennungen IMSI/IMEI haben im Bereich der mobilen Telekommunikation für die Mobilfunkteilnehmer, aber auch für die Sicherheitsbehörden enorme Bedeutung. Grundsätzlich meldet sich jedes eingeschaltete und im Stand-by-Betrieb befindliche Mobiltelefon bei der Basisstation derjenigen Funkzelle an, in welcher es sich gerade befindet.[16] Hierbei werden die IMSI und IMEI übermittelt, um den Teilnehmer zu identifizieren.[17] Die Funksignale des Handys werden von der Basisstation an den jeweiligen Netzbetreiber weitergeleitet und von diesem gespeichert.[18] Somit ist eine durchgehende Erreichbarkeit des Teilnehmers gewährleistet.[19]

Sind diese Kennungen den Behörden bekannt, kann die zugehörige Rufnummer bei den Mobilfunkanbietern erfragt[20] und die mit dem entsprechenden Mobilfunkgerät geführte Telekommunikation überwacht werden.[21] Jedoch wechseln gerade im Bereich der organisierten Kriminalität die Teilnehmer zur Verschleierung häufig die Mobiltelefone und SIM-Karten untereinander aus oder benutzen durch Dritte abgeschlossene Mobilfunkverträge.[22] Eine lückenlose Telefonüberwachung ist bei fehlender Kenntnis der IMSI oder IMEI nicht möglich.

c) Funktionsweise des IMSI-Catchers

aa) Grundsätzliches

Der IMSI-Catcher ist ein technisches Gerät der deutschen Elektronikfirma Rhode und Schwarz. Er wurde im Dezember 1996 ursprünglich als Test- und Messsystem unter der Typenbezeichnung GA 090 konstruiert und später als GA 900 zur Bestimmung der Endgerätekennung von Mobilfunkgeräten weiterentwickelt.[23] Das Gerät hat etwa die Größe eines Personal Computers (PC) und besteht aus Steuerungsrechner, Antenne und Messgeräten.[24] Der IMSI-Catcher besitzt vier verschiedene Funktionsweisen. Mittels dieses Geräts können IMSI und IMEI eines Mobilfunkteilnehmers für anschließende Maßnahmen der Telekommunikationsüberwachung nach §§ 100a ff. StPO ermittelt werden. Sind diese bereits bekannt, ist auch die Lokalisierung eines empfangsbereiten Mobilfunkendgeräts möglich. Unter bestimmten Voraussetzungen können zudem Gespräche mitgehört werden.

bb) Ermittlung der IMSI

Die für die Praxis wichtigste Funktion stellt die Ermittlung fehlender IMSI zur anschließenden Telekommunikationsüberwachung dar. Erforderlich hierfür ist die Kenntnis vom Standort des "zu fangenden" Teilnehmers. Der IMSI-Catcher simuliert sodann in dessen unmittelbarer Nähe die Basisstation einer Funkzelle.[25] Da sich die Funkzellen benachbarter Sendemasten häufig überlappen, bucht sich das empfangsbereite Handy stets in die Funkzelle mit dem stärksten Signal ein.[26] Diesen Effekt

macht sich der IMSI-Catcher zunutze, indem er ein stärkeres Signal[27] erzeugt, als jenes der stärksten Funkzelle.[28] Alle empfangsbereiten Mobilfunkgeräte in einem bestimmten Umkreis, also auch das des gesuchten Teilnehmers, buchen sich sodann in die vermeintlich existierende Funkzelle ein.[29] Die Mobiltelefone werden auf diese Weise für ein paar Sekunden "gefangen" und anschließend wieder in die ursprüngliche Zelle entlassen.[30] Hierbei wird die IMSI an den IMSI-Catcher gesendet.

cc) Ermittlung der IMEI

Neben der IMSI schickt das eingeschaltete Mobiltelefon bei jedem Funkkontakt auch die IMEI-Kennung an die jeweilige Basisstation.[31] Diese Gerätenummer kann mithilfe des IMSI-Catchers auf ähnliche Weise ermittelt werden wie die IMSI.[32] Die Kenntnis dieser Nummer ist für die Strafverfolgungs- und Sicherheitsbehörden dann von Bedeutung, wenn der telekommunikativ zu überwachende Teilnehmer sich verschiedener SIM-Karten und somit verschiedener IMSI-Kennungen bedient. Über die IMEI kann eine Verbindung zwischen dem Endgerät und sämtlichen benutzten SIM-Karten hergestellt werden. Hierdurch ist es sodann möglich, die verschiedenen Rufnummern zu ermitteln. Die Behörden sind also selbst dann zu einer anschließenden Telekommunikationsüberwachung imstande, wenn die Software durch Austausch des SIM häufig gewechselt wird.[33]

dd) Standortbestimmung

Sind IMSI oder IMEI bereits bekannt, kann mittels des IMSI-Catchers auch der Standort des Geräts bzw. der eingesetzten SIM-Karte bestimmt werden (Ortung). Voraussetzung hierfür ist jedoch eine grobe Kenntnis vom Aufenthaltsort der gesuchten Person. Soweit sich das gesuchte Mobilfunktelefon im Stand-By-Modus befindet, kann die Lokalisierung innerhalb des Netzes bereits durch den Mobilfunkanbieter vorgenommen werden, wobei die aktuelle Funkzelle und somit der grobe Standort des Mobilfunkgeräts erkennbar ist.[34] Die Genauigkeit dieser Standortbestimmung richtet sich wiederum nach der Größe der jeweiligen Funkzelle,[35] so dass die gesuchte Person bis auf ca. 30 Meter genau geortet werden kann.[36] Eine genauere Lokalisierung des Handy-Nutzers ist nur durch den Einsatz des IMSI-Catchers möglich.[37] Dies geschieht in der Weise, dass das Gerät eine Funkzelle mit geringerer Leistung und somit geringerer geographischer Ausdehnung simuliert.[38] Das gesuchte Mobilfunktelefon bucht sich nur dann in diese "Funkzelle" ein, soweit sich diese wegen ihres schwachen Signals in unmittelbarer Nähe befindet. Es werden mehrere Peilungen von verschiedenen Standorten aus durchgeführt, wodurch der Aufenthaltsort der gesuchten IMSI/IMEI stark eingegrenzt werden kann.[39] Die praktische Relevanz dieser Funktion könnte jedoch aufgrund neuer technischer Möglichkeiten bald der Vergangenheit angehören.[40]

ee) Abhören von Gesprächsinhalten

Der IMSI-Catcher bietet bei etwas modifizierter Bauart zusätzlich die Möglichkeit, ausgehende Gespräche eines Mobilfunkgerätes, dessen IMSI/IMEI bekannt sind, direkt vor Ort abzuhören.[41] Er verhält sich hierbei gegenüber dem Mobilfunknetz selbst wie ein Mobilfunkgerät,[42] schaltet sich somit zwischen Mobilfunkgerät und Basisstation ein. Es handelt sich hierbei um einen so genannten "Man-in-the-middle"-Angriff. Der IMSI-Catcher leitet als Zwischenbasis die von dem gefangenen Handy ausgehenden Datenpakete an die Basisstation des Netzbetreibers weiter und umgekehrt.[43] Hierdurch ist ein unmittelbares Mithören der Inhalte abgehender Gespräche möglich. Eingehende Gespräche können hingegen nicht abgehört werden. Sie werden durch den IMSI-Catcher blockiert.[44] Im Gegensatz zum GA 090, dem Ursprungsmodell des IMSI-Catchers, verfügt der GA 900 bereits über eine solche Abhörfunktion durch eine entsprechend integrierte Zusatzsoftware.[45]

ff) Begleitumstände

Der Einsatz des IMSI-Catchers ist mit einigen negativen Begleitumständen verbunden. Durch die Simulation einer Basisstation buchen sich alle empfangsbereiten Mobiltelefone in der Umgebung beim IMSI-Catcher ein. In dieser Zeit haben die Geräte keine Verbindung zum regulären Netz, so dass derweil der Aufbau einer Telekommunikationsverbindung nicht möglich ist.[46] Betroffen sind sowohl abgehende als auch eingehende Gespräche und Kurzmitteilungen. Auch das Absetzen von Notrufen ist nicht möglich.[47] Die Dauer dieses Zustands wird unterschiedlich bewertet. Während die Bundesregierung von einer Störung in Höhe von zehn Sekunden ausgeht,[48] geben die Netzbetreiber, gestützt auf eine Information des Herstellers Rhode und Schwarz, einen Ausfall von mehreren Minuten an.[49] Der IMSI-Catcher kann zudem aufgrund seiner hohen Leistung zu erheblichen Netzstö-

rungen, bis hin zum Ausfall der Basisstation führen.[50] Aufgrund der Überlappung von echter und simulierter Funkzelle kann es durch Interferenzen zwischen der benutzten Frequenz des Geräts und den Funksignalen der echten Basisstation im Einzugsbereich des Catchers zu Gesprächsabbrüchen kommen.[51] Nicht zuletzt besteht eine Missbrauchsgefahr durch Dritte, die den IMSI-Catcher legal erwerben können. Das Gerät wird von der Firma Rhode und Schwarz auch ins Ausland exportiert. Aufgrund mangelnder technischer Nachweisbarkeit des Einsatzes entsprechender Geräte ist ein Missbrauch durch ausländische Geheimdienste oder kriminelle Vereinigungen zu befürchten.[52]

2. Rechtliche Grundlagen

Die rechtliche Grundlage für den hier zu untersuchenden Einsatz des IMSI-Catchers zu Strafverfolgungszwecken findet sich in § 100i StPO. Der IMSI-Catcher ist in seiner Anwendung aber keineswegs darauf beschränkt. Vielmehr besteht auch im Bereich der Gefahrenabwehr die Möglichkeit seines Einsatzes. Auf Bundesebene stellen die § 9 Abs. 4 BVerfSchG, § 3 BNDG und § 5 MADG entsprechende präventivgesetzliche Befugnisnormen dar. Sie erlauben dem Bundesamt für Verfassungsschutz, dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst im Rahmen ihrer jeweiligen Aufgabenwahrnehmung ausdrücklich den Einsatz technischer Mittel zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts und zur Ermittlung der Geräte- und Kartennummer. Bundespolizei und Bundeskriminalamt sind in ihrer Funktion als Strafverfolgungsbehörden nach § 100i StPO legitimiert. Über die Möglichkeit eines Einsatzes ausschließlich zu repressiven Zwecken hinaus stand ihnen bisher keine originäre Befugnis zum Präventiveinsatz des IMSI-Catchers zur Seite. Seit 1. Januar 2009 findet sich nunmehr in § 20n BKAG[53] eine entsprechende Spezialbefugnis, die es dem BKA ermöglicht, sich im Rahmen der ihm zugewiesenen Gefahrenabwehraufgaben (Abwehr von Gefahren des internationalen Terrorismus nach § 4a BKAG) des IMSI-Catchers zu bedienen.

Und auch die Landespolizei hat in zahlreichen Bundesländern die Möglichkeit, den IMSI-Catcher unter bestimmten Voraussetzungen einzusetzen. Regelungen hierzu finden sich in § 25a Abs. 2 ASOG Bln., § 33b Abs. 3 BbgPolG, § 34a Abs. 2 BayPAG, § 33 Abs. 1 BremPolG, § 23a Abs. 6 BWPolG, § 10b Abs. 3 HmbDVPolG, § 15a Abs. 3 HSOG, § 185a Abs. 3 LVwG SH, § 33b Abs. 1 Nds.SOG, §§ 28 Abs. 2, 31 Abs. 2 POG RP, § 34a Abs. 2, 3 SOG MV, § 28b Abs. 4 SPolG und § 34a Abs. 2 ThürPAG.

III. Repressive Einsatzmöglichkeit

Der Einsatz des IMSI-Catchers im Rahmen der Strafverfolgung ist heute unter den Voraussetzungen des § 100i StPO zulässig.

1. Entstehungsgeschichte des § 100i StPO

Der Einführung des § 100i StPO gingen kontroverse Diskussionen in der Öffentlichkeit sowie unterschiedliche, voneinander unabhängige Gesetzgebungsbestrebungen voraus. Strafverfolgungs- und Sicherheitsbehörden sowie Teile der Rechtsprechung gingen gar davon aus, dass die vor 2002 geltende Rechtslage den Einsatz des IMSI-Catchers zur Ermittlung der Mobilfunkgerätekennungen ermöglichen würde.

a) Gesetzliche Grundlagen vor dem Jahr 2002

So vertrat etwa die Bundesregierung die Auffassung, der Einsatz des IMSI-Catchers zu repressiven Zwecken sei durch §§ 100a ff., 161 StPO a.F. gedeckt. § 161 StPO a.F. erlaube den Strafverfolgungsbehörden, *Ermittlungen jeder Art* anzustellen, um einen Sachverhalt zu erforschen. Als allgemeine Generalermittlungsklausel räume diese Vorschrift den Behörden auch die Möglichkeit ein, mittels des Einsatzes eines IMSI-Catchers die Voraussetzungen für die Wahrnehmung ihrer Spezialbefugnisse nach §§ 100a ff. StPO zu schaffen.[54]

Diskutiert wurde zudem ein Rückgriff allein auf die Befugnisnorm des § 100a StPO, welcher die Überwachung und Aufzeichnung

der Telekommunikation regelt.[55] Teile der Rechtsprechung sahen in der IMEI lediglich eine *andere Kennung* i.S. des § 100b Abs. 2 S. 2 StPO a.F.,[56] welche den Bezugspunkt für eine Telefonüberwachung bietet. Zudem würde § 100a StPO die Ermittlung von Standortdaten selbst dann erfassen, wenn sich das Mobiltelefon im Stand-by-Modus befindet. Nach dieser Ansicht konnte, sofern IMSI oder IMEI bekannt waren und auch die übrigen Voraussetzungen des § 100a StPO vorlagen, sogar eine Standortbestimmung mittels IMSI-Catcher über § 100a StPO durchgeführt werden.[57]

Gestützt auf eine Entscheidung des AG München aus dem Jahre 2001, ging eine andere Ansicht davon aus, dass der Einsatz des IMSI-Catchers nach § 100c Abs. 1 Nr. 1 lit. b StPO a.F. möglich sei.[58] Diese Vorschrift betraf die Zulässigkeit des Einsatzes sonstiger für Observationszwecke bestimmter technischer Mittel. Aus der permanenten Ortungsmöglichkeit eines Mobiltelefons mittels eines IMSI-Catchers folgerte die genannte Ansicht, dass es sich dabei um eben ein solches technisches Mittel i.S. des § 100c Abs. 1 Nr. 1 lit. b StPO a.F. handele.[59]

Strafverfolgungs- und Sicherheitsbehörden hingegen, welche zwischen 1998 und 2001 den IMSI-Catcher bereits 35-mal eingesetzt haben,[60] beriefen sich zu ihrer Rechtfertigung auf die Notstandsregelung des § 34 StGB.[61] Unabhängig von der höchst problematischen Streitfrage, ob sich staatliche Organe überhaupt auf allgemeine Notstandsregelungen des StGB berufen können, bestünde bei einer Anwendung des § 34 StGB in derartigen Konstellationen die Gefahr, dass zentrale verfassungsrechtliche Erfordernisse umgangen werden könnten. § 34 StGB genügt nicht den Anforderungen an das grundgesetzlich verankerte Prinzip des Gesetzesvorbehalts, das bei Grundrechtseingriffen eine nach Inhalt, Zweck und Ausmaß hinreichend bestimmte gesetzliche Ermächtigung verlangt. Zudem tragen die auf das Bürger-Bürger-Verhältnis zugeschnittenen allgemeinen Rechtfertigungsgründe des StGB nicht den verfassungsrechtlichen Erfordernissen des Übermaßverbots sowie den sonstigen grundrechtlichen Beschränkungen staatlichen Handelns Rechnung. Hinzu kommt, dass ein Rückgriff auf § 34 StGB ohnehin lediglich die Abwehr einer Gefahr erlaubt, nicht aber repressive Maßnahmen decken würde.

Die herrschende Ansicht in der Literatur ging daher im Ergebnis zu Recht davon aus, dass eine Rechtsgrundlage bis zur Einführung des § 100i StPO gar nicht existierte und der Einsatz des IMSI-Catchers nach der bis dahin geltenden Rechtslage gegen das Grundgesetz verstieß.[62]

b) Stationen des Gesetzgebungsverfahrens

Bereits im Sommer 1997 wurde der Ruf nach einer gesetzlichen Regelung zum repressiven Einsatz des IMSI-Catchers laut. Im Zusammenhang mit der Diskussion über den Gesetzentwurf der Bundesregierung für ein Begleitgesetz zum Telekommunikationsgesetz[63] forderte der Bundesrat die Bundesregierung im Rahmen eines Änderungsvorschlags dazu auf, eine gesetzliche Regelung zu schaffen.[64] Diese Vorschläge führten auch im weiteren Gesetzgebungsverfahren zu einer regen Diskussion,[65] wurden aber letztendlich nicht Gegenstand des Begleitgesetzes. Die Bundesregierung stand der Schaffung einer speziellen Befugnisnorm ablehnend gegenüber. Das Interesse am Einsatz des IMSI-Catchers riss dagegen nicht ab.[66] Einen erneuten Impuls erhielt das Gesetzgebungsverfahren allerdings erst durch einen Gesetzentwurf der Bundesregierung vom 23. November 2001, der eine Änderung der Strafprozessordnung, insbesondere des § 81f StPO, zum Inhalt hatte.[67] Der Rechtsausschuss des Bundestags implementierte in seiner Beschlussempfehlung im Anschluss an eine Sachverständigenanhörung zusätzlich eine Regelung zum Einsatz des IMSI-Catchers. Dieser sollte aus Gründen der Rechtssicherheit und Rechtsklarheit auf eine solide gesetzliche Grundlage gestellt werden.[68] Diese Beschlussempfehlung wurde unverändert und ohne vorherige Aussprache vom Bundestag angenommen und als Gesetz beschlossen.[69] Das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 und mit ihm der neue § 100i StPO a.F. konnten somit am 14. August 2002 in Kraft treten.[70]

c) Novelle zum 1. Januar 2008

Nach kleineren, formellen Änderungen des § 100i StPO a.F.[71] kam es zum 1. Januar 2008 zu einer kompletten Novellierung der strafprozessualen verdeckten Ermittlungsmaßnahmen und der Telekommunikationsüberwachung. Am 27. Juni 2007 legte die Bundesregierung dem Bundestag den *Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* vor. Dieser sah eine grundlegende Änderung der Regelungen in den §§ 100a ff. StPO vor. Auch § 100i StPO sollte im Zuge der Novelle neu gefasst werden. Der Gesetzgeber wollte dabei vor allem die in § 100g Abs. 1 S. 1 StPO bereits verankerte materielle Schwelle einer *Straftat von erheblicher Bedeutung* integrieren. Durch den Fortfall der strengen Zweckbindung soll der Einsatz zudem von der Anordnung einer Telekommunikationsüberwachung entkoppelt werden und auch im Rahmen einer Verkehrsdatenerhebung nach § 100g StPO oder zur Unterstützung von Observationsmaßnahmen zulässigerweise angeordnet werden können.[72] Das Gesetz wurde am 9. November 2007 vom Bundestag beschlossen und trat zum 1. Januar 2008 in Kraft.

2. Voraussetzungen nach § 100i StPO

a) Materielle Voraussetzungen

Die materiellen Voraussetzungen des Einsatzes eines IMSI-Catchers finden sich nunmehr zusammengefasst im ersten Absatz des § 100i StPO. Die Vorschrift erlaubt unter nachfolgend erläuterten Voraussetzungen dessen Einsatz zur Ermittlung der IMSI/IMEI sowie zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunk-

endgeräts. Technisch mögliche Abhörmaßnahmen dürfen jedoch nicht auf § 100i StPO gestützt werden. Sie sind nur unter den qualifizierten Voraussetzungen der §§ 100a f. StPO zulässig.

aa) Straftat von erheblicher Bedeutung

Anknüpfungspunkt einer Maßnahme nach § 100i StPO ist, wie bei jeder strafprozessualen Maßnahme, das Vorliegen eines Anfangsverdachts bezüglich einer Straftat. Darüber hinaus muss jedoch ein weiteres, qualifiziertes Erfordernis verwirklicht sein. Der Verdacht darf sich nicht, wie bei den meisten Ermittlungsmaßnahmen ausreichend, auf jedwede Straftat beziehen. Vielmehr müssen bestimmte Tatsachen vorliegen, die die Annahme einer Straftat von auch im Einzelfall erheblicher Bedeutung rechtfertigen. Eine Straftat von erheblicher Bedeutung liegt vor, wenn sie mindestens dem Bereich der mittleren Kriminalität zuzuordnen ist, den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[73] Hierbei kommen insbesondere – jedoch nicht abschließend – Katalogtaten nach § 100a Abs. 2 StPO in Betracht. Die Tat kann sowohl vollendet als auch versucht sein. Auch Vorbereitungshandlungen zu einer erheblichen Straftat oder die Teilnahme daran eröffnen, soweit es sich hierbei um eine eigenständige Straftat handelt, die Möglichkeit eines Einsatzes.[74] Erforderlich ist jedoch stets, dass die Taten auch im Einzelfall und nicht nur abstrakt von erheblicher Bedeutung sind. Daher ist in jedem Fall eine einzelfallbezogene Beurteilung des Tatgeschehens unter Berücksichtigung des allgemeinen Verhältnismäßigkeitsprinzips vorzunehmen.[75]

Die Vorschrift des § 100i StPO a.F. hat hingegen noch differenziert. Die Ermittlung der Geräte- und Kartennummer nach § 100i Abs. 1 Nr. 1 StPO a.F. hat stets erfordert, dass die Voraussetzungen des § 100a StPO vorliegen (§ 100i Abs. 2 S. 1 StPO a.F.). Dies bedeutete insbesondere das Vorliegen eines qualifizierten Anfangsverdachts bezüglich einer der in § 100a StPO abschließend aufgezählten Katalogtaten.[76] Eine Maßnahme nach § 100i Abs. 1 Nr. 2 StPO a.F. zur Standortermittlung hat hingegen einen Anfangsverdacht hinsichtlich einer Straftat von erheblicher Bedeutung genügen lassen (§ 100i Abs. 2 S. 2 StPO a.F.).[77]

Der Gesetzgeber hat mit der Neuregelung des § 100i StPO die Anforderungen an die Ermittlung der Geräte- und Kartennummer insgesamt gesenkt, indem nun nicht mehr der abschließende Straftatenkatalog nach § 100a StPO zu Grunde zu legen ist.

bb) Zweckbindung

Der Einsatz des IMSI-Catchers erfolgt zum Zwecke der Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts des Beschuldigten. Die Maßnahmen nach § 100i StPO unterliegen demnach keiner weiteren, die Wahrnehmung des strafprozessualen Untersuchungsgrundsatzes[78] (§ 160 Abs. 1 StPO) einschränkenden Zweckbindung. Insbesondere dürfen sowohl die Kennungen als auch der Standort des Mobilfunkteilnehmers zur Unterstützung einer Observationsmaßnahme sowie zur Vorbereitung einer Verkehrsdatenerhebung nach § 100g StPO ermittelt werden.[79] Auch die Ermittlung von IMSI/IMEI mit dem Ziel einer späteren Durchführung der Standortermittlung ist im Unterschied zur alten Regelung nunmehr möglich.

Im Gegensatz dazu waren die Maßnahmen nach § 100i StPO a.F. streng zweckgebunden.[80] Die Ermittlung der Geräte- und Kartennummer war ausschließlich zum Zwecke der Vorbereitung einer Maßnahme nach § 100a StPO zulässig (§ 100i Abs. 1 Nr. 1 StPO a.F.). Die Standortermittlung nach § 100i Abs. 1 Nr. 2 StPO a.F. war nur zur vorläufigen Festnahme (§ 127 Abs. 2 StPO) oder zur Ergreifung des Beschuldigten aufgrund eines Haftbefehls (§ 114 StPO) oder eines Unterbringungsbefehls (§ 126a StPO) möglich. Ausnahmsweise durfte eine Standortbestimmung auch durchgeführt werden, soweit dies zur Eigensicherung der zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich war (§ 100i Abs. 2 S. 3 StPO a.F.).[81]

Der Gesetzgeber hat durch die Streichung der strengen Zweckbindung den Anwendungsbereich des § 100i StPO erheblich erweitert.

cc) Zielperson der Maßnahme

Die Maßnahmen nach § 100i Abs. 1 StPO dürfen sich nur gegen die in § 100i Abs. 3 S. 1 i.V.m. § 100a Abs. 3 StPO genannten Personen richten. In erster Linie kommt natürlich der Beschuldigte als von der Maßnahme Betroffener in Betracht. Beschuldigte in diesem Sinne sind nach § 100i Abs. 1 StPO Täter oder Teilnehmer der Straftat von erheblicher Bedeutung sowie Personen, welche diese Straftat durch eine andere, eigenständige Straftat vorbereitet haben. Weiterhin dürfen sich die Maßnahmen auch gegen sog. Kontaktpersonen, insbesondere Nachrichtenmittler, richten, also diejenigen Personen, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben

oder dass der Beschuldigte ihren Anschluss benutzt.

Nach der bis zum 31. Dezember 2007 geltenden Rechtslage bestimmte sich die Zielperson jeweils nach der Zweckrichtung der Maßnahme. Im Falle des § 100i Abs. 1 Nr. 1 StPO a.F. war die Zielperson der Täter oder Teilnehmer der Katalogtat nach § 100a StPO sowie derjenige, der diese durch eine Straftat vorbereitet hat. Die Maßnahme durfte zudem gegen sog. Nachrichtenmittler im Sinne des § 100a S. 2 StPO a.F. durchgeführt werden. Nach § 100i Abs. 1 Nr. 2 StPO a.F. war Zielperson[82] derjenige Beschuldigte, gegen den sich die vorläufige Festnahme bzw. der Haft- oder Unterbringungsbefehl richtete. Auch diese Maßnahme war gegen andere Personen (Kontaktpersonen) zulässig, wenn die Ermittlung des Aufenthaltsorts des Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert gewesen wäre (§§ 100i Abs. 2 S. 2 a.E., 100f Abs. 3 S. 2 StPO a.F.).[83] Zur Bestimmung des Aufenthaltsorts waren Ermittlungen gegen Dritte damit nach früherer Rechtslage nur unter Beachtung der qualifizierten Subsidiaritätsklausel möglich. Diese Hürde hat der Gesetzgeber nunmehr mit Verweis auf die Neuregelung in § 100a Abs. 3 StPO, die keine Subsidiaritätsklausel enthält, genommen.

dd) Subsidiaritätsklausel

Bei der Neuregelung des § 100i StPO hat der Gesetzgeber auf eine Subsidiaritätsklausel, wie sie vorher bestand, verzichtet. Die nunmehr ausdrücklich normierte Beschränkung des Einsatzes von IMSI-Catchern auf solche Fälle, in denen ein entsprechender Einsatz *erforderlich* ist, stellt hingegen keine Subsidiaritätsklausel im eigentlichen Sinne und keine wirkliche Verengung des Anwendungsbereichs dar. Es handelt sich vielmehr lediglich um einen Ausfluss aus dem ohnehin geltenden Verhältnismäßigkeitsprinzip.

Die Vorgängerregelung in § 100i StPO a.F. differenzierte hingegen noch. Die Maßnahme nach § 100i Abs. 1 Nr. 1 StPO a.F. war streng subsidiär.[84] Hiernach durften Geräte- und Kartennummer mittels IMSI-Catcher nur erhoben werden, wenn die Durchführung der Überwachungsmaßnahme ohne die Ermittlung der entsprechenden Kennungen nicht möglich oder wesentlich erschwert gewesen wäre. Diese Maßnahme unterlag, da zudem die Voraussetzungen nach § 100a StPO vorliegen mussten, sogar einer doppelten Subsidiaritätsklausel.[85] Der Einsatz des IMSI-Catchers nach § 100i Abs. 1 Nr. 2 StPO a.F. war hingegen bereits dann zulässig, wenn die Ermittlung des Aufenthaltsorts des Täters auf andere Weise weniger erfolgversprechend oder erschwert gewesen wäre.[86]

b) Anordnungsvoraussetzungen

Die Verfahrensvoraussetzungen finden sich nunmehr in § 100i Abs. 3 StPO. Die Maßnahme nach Abs. 1 bedarf grundsätzlich der Anordnung durch den Richter auf Antrag der Staatsanwaltschaft. Lediglich bei Gefahr im Verzug kann die Staatsanwaltschaft die Anordnung eigenständig treffen. Diese muss jedoch anschließend binnen dreier Werktage von einem Gericht bestätigt werden, anderenfalls tritt sie außer Kraft (§ 100i Abs. 3 S. 1 i.V.m. § 100b Abs. 1 S. 1 bis 3 StPO). Die Anordnung ergeht gemäß § 100i Abs. 3 S. 1 i.V.m. § 100b Abs. 2 S. 1 StPO schriftlich. Sie darf auf höchstens sechs Monate begrenzt werden (§ 100i Abs. 3 S. 2 StPO). Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist nur zulässig, soweit die Voraussetzungen nach Abs. 1 weiterhin vorliegen (§ 100i Abs. 3 S. 3 StPO). Fallen diese hingegen während des Vollzugs der Maßnahme weg, so ist der Vollzug sofort zu beenden (§ 100i Abs. 3 S. 1 i.V.m. § 100b Abs. 4 S. 1 StPO). Gemäß § 101 Abs. 4 S. 1 Nr. 8 StPO ist der Betroffene nach Beendigung der Maßnahme zu benachrichtigen.

c) Verwendung der Daten des Betroffenen

Die erhobenen Daten des Betroffenen dürfen nach § 100i Abs. 1 StPO zur Ermittlung des Sachverhalts und der Bestimmung des Aufenthaltsorts verwendet werden. Beweisverwertungsverbote bestehen im Rahmen der allgemeinen Grundsätze. Die Verwendung der Daten zu Beweiszwecken in anderen, unabhängig von der Anlasstat bestehenden Strafverfahren ist unter den besonderen Voraussetzungen der Verwendungsregelung des § 477 Abs. 2 S. 2 StPO zulässig. Dieser gesetzlichen Regelung bezüglich sog. Zufallsfunde liegt der Gedanke des hypothetischen Ersatzeingriffs zugrunde.[87] Zu präventivpolizeilichen Zwecken dürfen die nach § 100i StPO erhobenen Daten nur unter den Voraussetzungen des § 477 Abs. 2 S. 3 StPO verwendet werden; also etwa zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit. Für den Fall, dass die erhobenen Daten für die Strafverfolgung oder die gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich sind, enthält § 101 Abs. 8 StPO eine Löschungspflicht. Eine Kennzeichnungspflicht ergibt sich aus § 101 Abs. 3 StPO. Handelt es sich bei der von der Maßnahme betroffenen Zielperson, sofern nicht Beschuldigter,[88] um einen zeugnisverweigerungsberechtigten Berufsgeheimnisträger, so ergeben sich aus § 160a Abs. 1 S. 1 bis 4, Abs. 2 StPO Beweiserhebungs- und Beweisverwendungsverbote (einschließlich eines Verwertungsverbots) sowie Dokumentations- und Löschungspflichten.

d) Personenbezogene Daten Dritter

In § 100i Abs. 2 StPO findet sich eine Regelung bezüglich der erhobenen personenbezogenen Daten Dritter. Funktionsbedingt meldet sich beim Einsatz des IMSI-Catchers jedes Mobiltelefon in dessen Umgebung bei dieser vermeintlichen Funkzelle bzw. deren vermeintlicher Basisstation an und übermittelt hierbei seine Geräte- und Kartennummer. Es werden damit auch Kennungen unbeteiligter Dritter ermittelt. Dies wird, soweit es aus technischen Gründen unvermeidbar ist, als zulässig und mit dem Grundgesetz vereinbar angesehen.[89] In der Regel werden jedoch die Daten von Mobiltelefonen Dritter schon durch die Bildung von Schnittmengen aus den Daten mehrerer Messungen wieder ausgeschieden.[90] Dennoch erhobene Daten dürfen jedoch nach § 100i Abs. 2 S. 2 StPO ausschließlich zum Zwecke des Datenabgleichs zur Ermittlung der gesuchten Geräte- und Kartennummer verwendet werden. Dieser Datenabgleich erfolgt über den Netzbetreiber, welcher in Kenntnis der IMSI/IMEI den gesuchten Teilnehmer sowie dessen Mobilfunk-Rufnummer identifizieren kann. Über diesen Datenabgleich hinaus dürfen die Kennungen Dritter nicht verwendet werden (Verbot der Zweckänderung).[91] Die Regelungen des § 477 Abs. 2 S. 2 und 3 StPO finden keine Anwendung. § 100i Abs. 2 S. 2 StPO, der insoweit ein absolutes Verwendungsverbot[92] für Zufallsfunde hinsichtlich personenbezogener Daten Dritter normiert, ist lex specialis (vgl. § 477 Abs. 2 S. 4 StPO). Nach Beendigung der Maßnahme sind die Daten unverzüglich zu löschen (§ 100i Abs. 2 S. 2 StPO). Handelt es sich bei dem Dritten um einen zeugnisverweigerungsberechtigten Berufsgeheimnisträger, so ergeben sich Beweisverwendungsverbote sowie Dokumentations- und Löschungspflichten aus § 160a Abs. 1 S. 5 StPO. Aus dieser Vorschrift kann sich über die in § 100i Abs. 2 StPO normierten Pflichten hinaus in Einzelfällen unter Anwendung des Grundsatzes der Verhältnismäßigkeit sogar ein ungeschriebenes relatives Beweiserhebungsverbot mit der Verpflichtung ergeben, die Maßnahme zu unter- bzw. abzubrechen.[93]

3. Bedeutung der gesetzlichen Regelung

Mit der in § 100i StPO vorgesehenen Befugnis hat der Gesetzgeber den Strafverfolgungsbehörden ein Instrument an die Hand gegeben, sich durch Ermittlung von IMSI und IMEI die für die Anordnung einer Telekommunikationsüberwachung notwendigen Informationen zu beschaffen. Darüber hinaus wurden mit der Regelung die Möglichkeiten der Strafverfolgungsbehörden erweitert,

den Aufenthaltsort eines Beschuldigten zu ermitteln. Neben der angemahnten verfassungsrechtlichen Notwendigkeit der Schaffung einer gesetzlichen Grundlage wurde die Implementierung des § 100i StPO im Jahre 2002 in weiten Teilen als notwendiger Reflex auf technische Entwicklungen begrüßt.[94] Gleichwohl sind mit dem Einsatz des IMSI-Catchers auch eine Reihe von technisch bedingten Einschränkungen verbunden, die ihrerseits die Ermittlungstätigkeit begrenzen. Zunächst ergibt sich das generelle Problem, dass alle mittels des IMSI-Catchers durchgeführten Maßnahmen voraussetzen, dass der Aufenthaltsort des Betroffenen aufgrund von Observationen oder einer Funkzellenabfrage grob bestimmbar ist. Das zu ermittelnde Gerät muss zudem aktiv geschaltet sein, sich also im Stand-by-Modus befinden. Um anschließend die gesuchte IMSI oder IMEI herausfiltern zu können, sind oftmals mehrere Messungen erforderlich.[95]

Problemlagen haben sich jedoch nicht nur aus den technischen Gegebenheiten, sondern auch aus der unstrukturierten und inkohärenten Gesetzessystematik ergeben, deren Bereinigung und Harmonisierung zentrales gesetzgeberisches Anliegen der Novellierung der §§ 100a ff. StPO zum 1. Januar 2008 war. So hat etwa § 100i StPO a.F. die Ermittlung der Gerätenummer IMEI mittels des IMSI-Catchers ausdrücklich zugelassen; jedoch war streitig, ob mittels dieser Kennung anschließend die Überwachung der Telekommunikation angeordnet werden konnte.[96] Der Gesetzgeber hat diese Unklarheit nun behoben, indem er in § 100b Abs. 2 Nr. 2 StPO n.F. auch die Kennung des Endgeräts ausdrücklich erwähnt. Die Ermittlung der IMEI hat durch diese Klarstellung[97] an praktischer Bedeutung gewonnen.

Die praktische Relevanz der Standortermittlung mittels IMSI-Catcher hat hingegen nachgelassen. Hier muss zunächst IMSI/IMEI des zu ortenden Teilnehmers bekannt sein. Zudem muss dessen Aufenthaltsort eng eingegrenzt werden. All dies macht die Ortung mittels IMSI-Catcher unpraktikabel. In der Praxis wurde er mittlerweile bereits durch die Ermittlungsmaßnahme der sog. *stillen SMS* abgelöst.[98] Hierbei handelt es sich um ein Signal, welches von den Ermittlern durch ein einfaches Computerprogramm oder per Handy an eine ihnen bekannte Mobilfunk-Rufnummer gesandt wird.[99] Diese SMS (Short Message Service) ist für den Besitzer des Mobiltelefons nicht wahrnehmbar, erzeugt beim Mobilfunkbetreiber

jedoch künstlich Verbindungsdaten, welche von den Strafverfolgungsbehörden abgerufen werden können.[100] Hierdurch kann die Funkzelle ermittelt werden, in der das Mobilfunkgerät gerade eingebucht ist,[101] ohne dass sich die Ermittlungsbeamten in unmittelbarer Nähe aufhalten müssen. Eine weitere, ebenfalls praktisch sehr bedeutsame Ermittlungsmethode stellt die auf § 100h Abs. 1 S. 1 Nr. 2 StPO gestützte Peilung via GPS dar.[102]

Insgesamt bleibt jedoch festzuhalten, dass der IMSI-Catcher und mit ihm die Rechtsgrundlage in § 100i StPO auch durch neue technische Entwicklungen nicht nennenswert an Bedeutung verloren haben.[103] Die Hauptfunktion des Geräts liegt bei der Ermittlung der IMSI. Gerade in diesem Bereich ist es mangels adäquater Alternativen sehr praxisrelevant.[104]

4. Zusammenfassung

Zusammenfassend kann festgestellt werden, dass der Gesetzgeber durch die Neuregelung der Befugnisnorm des § 100i StPO die Eingriffsschwelle vereinheitlicht und abgesenkt hat.[105] Durch den Wegfall der Subsidiaritätsklauseln und der Erweiterung des Straftatenkatalogs ist der Einsatz des IMSI-Catchers nun auch außerhalb des Anwendungsbereichs der Telekommunikationsüberwachungsmaßnahmen zulässig. Die Straffung und klarere Konturierung des Gesetzestextes haben darüber hinaus zu einer besseren Verständlichkeit und Übersichtlichkeit beigetragen.

IV. Verfassungsrechtliche Fragen

Wie jede staatliche Zwangsmaßnahme muss auch der Einsatz des IMSI-Catchers verfassungsrechtlichen Grundsätzen genügen und insbesondere dem Grundsatz der Verhältnismäßigkeit Rechnung tragen.

1. Grundrechtsbetroffenheit

Die den Einsatz des IMSI-Catchers legitimierende Norm steht im Kontext der Telekommunikationsüberwachungsmaßnahmen. Aufgrund dieser systematischen Stellung scheint ein Eingriff in das durch Art. 10 Abs. 1 Var. 3 GG geschützte Fernmeldegeheimnis nahe liegend. Auch das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG sowie die Meinungsfreiheit gemäß Art. 5 Abs. 1 S. 1 Hs. 1 GG und die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG könnten betroffen sein.

a) Fernmeldegeheimnis

Das Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG erweitert das in Art. 10 Abs. 1 GG ebenfalls geschützte Brief- und Postgeheimnis. Schutzgut des Art. 10 GG ist zunächst die Vertraulichkeit der individuellen Kommunikation mittels bestimmter Übertragungsmedien.[106] Das Fernmeldegeheimnis knüpft speziell an die fernmeldetechnisch vermittelte Übertragung von Informationen, d.h. an den Fernmeldeverkehr, an.[107]

aa) Grundsätzliches

Fernmeldetechnische Medien sind besonders der Gefahr eines unkontrollierten Zugriffs durch unbefugte Dritte ausgesetzt. In der heutigen Informationsgesellschaft, in der Kommunikation zunehmend als Telekommunikation über eine räumliche Distanz stattfindet, soll das Fernmeldegeheimnis die Privatheit und die Vertraulichkeit der Kommunikation gewährleisten.[108] Die Kommunikationsteilnehmer sollen so gestellt werden, wie sie stünden, wenn die Kommunikation ohne fernmeldetechnische Mittel, also unter Anwesenden, stattfände.[109] Das Fernmeldegeheimnis schützt daher die körperlose Übermittlung von Informationen[110] mittels drahtloser oder drahtgebundener elektromagnetischer Wellen.[111] Der Schutzbereich des Art. 10 Abs. 1 GG ist aufgrund der rasanten technischen Entwicklungen im Bereich der Telekommunikation entwicklungsoffen.[112] Geschützt

sind nicht nur der traditionelle Telefon-, Telefax-, Telegramm- und Funkverkehr, sondern auch neuere elektronische Übertragungsmöglichkeiten wie Mobilfunk und E-Mail-Verkehr via Internet.[113]

Inhaltlich umfasst das Fernmeldegeheimnis den Schutz der Individualkommunikation gegen unbefugte Kenntnisnahme Dritter.[114] Dies beinhaltet zunächst den Schutz

von Kommunikationsinhalten,[115] also aller mittels Funktechnik ausgetauschten Informationen. Darüber hinaus wird auch die Vertraulichkeit der Kommunikationsumstände gewährleistet.[116] Dieser Schutz bezieht sich sowohl auf die Tatsache, dass überhaupt Kommunikation stattfindet, als auch auf deren Teilnehmer, Anschlüsse und Rufnummern.[117] Auch Häufigkeit, jeweiliger Zeitpunkt der Telekommunikation sowie Kommunikationsversuche zählen hierzu.[118]

bb) Übertragung der IMSI/IMEI-Kennung und Positionsmeldungen

Im Folgenden wird zu erörtern sein, ob mit dem Einsatz des IMSI-Catchers der Schutzbereich des Fernmeldegeheimnisses betroffen ist. Mobiltelefone stellen, wie oben festgestellt, ein geeignetes Übertragungsmittel i. S. des von Art. 10 Abs. 1 Var. 3 GG geschützten Fernmeldeverkehrs dar. Allerdings ist fraglich, ob es sich bei der Übertragung der IMSI/IMEI-Kennungen an die jeweilige Basisstation um eine durch Art. 10 Abs. 1 GG geschützte Kommunikation handelt. Ein hierzu ergangener Kammerbeschluss des BVerfG vom 22. August 2006,[119] in dem es ein Eingreifen des Art. 10 Abs. 1 GG verneinte, vermag eine abschließende Klärung nicht herbeizuführen. Denn es handelt sich hierbei um einen Nichtannahmebeschluss nach § 93b S. 1 BVerfGG, mit dem keine Entscheidung in der Sache erging und der als bloße Prozessentscheidung weder materielle Rechtskraft noch eine Bindungswirkung nach § 31 Abs. 1 BVerfGG entfaltet.[120]

Bezogen auf den Fernmeldeverkehr stellt das Fernmeldegeheimnis des Art. 10 Abs. 1 GG nach allgemeiner Auffassung eine spezielle Ausprägung des Rechts auf informationelle Selbstbestimmung dar[121] und soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen, um gerade den Gefahren zu begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben.[122] Es knüpft also an das Kommunikationsmedium an.[123] Ob die Datenerhebung nach § 100i StPO die Vertraulichkeit des Kommunikationsinhalts oder des Kommunikationsvorgangs betrifft, erscheint fraglich. Um nämlich den Schutz des Fernmeldegeheimnisses zu genießen, müsste es sich bei IMSI- und IMEI-Kennung um personen- und kommunikationsbezogene Daten handeln. Kommunikation setzt nach allgemeinem Sprachgebrauch eine Verständigung zwischen Menschen oder zumindest einen menschlich veranlassten Datenaustausch voraus.[124] Die wohl überwiegende Auffassung sieht in den sich regelmäßig wiederholenden Positionsmeldungen des Mobiltelefons und der damit einhergehenden Sendung von IMSI bzw. IMEI an die Basisstation einen solchen menschlich veranlassten Datenaustausch und hält den Schutzbereich des Art. 10 Abs. 1 GG damit für eröffnet.[125] Der Besitzer eines Mobiltelefons schalte dieses ausschließlich aktiv, um die technischen Voraussetzungen für eine erfolgreiche Kommunikation zu schaffen.[126] Er versetze das Mobiltelefon in Kommunikationsbereitschaft, wodurch er auch seine eigene Empfangsbereitschaft signalisiere.[127] Diese bloße Kommunikationsbereitschaft stelle einen näheren Umstand der Kommunikation dar und unterfalle daher dem Schutzbereich des Art. 10 Abs. 1 GG. Schließlich würde dadurch auch die Information, dass sich die betreffende Person für eine Kommunikation bereithält, geschützt.[128] Das Fernmeldegeheimnis diene der Ausschaltung von Gefahren für Kommunikationsinhalt und -vorgang, welche durch die zwangsweise Vermittlung von Dritten drohen.[129] Mit der strafprozessualen Möglichkeit, IMSI und IMEI zu ermitteln, würde der Nutzer aber gerade nicht denselben Schutz seiner Privatsphäre genießen, der ohne das Kommunikationsmedium bestünde.[130] Im Sinne eines möglichst umfassenden Grundrechtsschutzes soll auch dem Besitzer eines bloß aktiv geschalteten Mobiltelefons daher der Schutz des Fernmeldegeheimnisses gewährt werden.[131]

Dieser Auffassung ist jedoch entgegenzuhalten, dass der Datenaustausch in der vorliegenden Konstellation ausschließlich zwischen technischen Geräten stattfindet und folglich keine individuellen oder kommunikativen Züge trägt.[132] Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhal-

te bezieht und dem Kommunikationsbegriff immanent ist. Die bloße technische Eignung eines Geräts, als Kommunikationsmittel verwandt zu werden, sowie die vom Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft stellen noch keine Kommunikation dar.[133] Daran ändert auch der Umstand nichts, dass es der Nutzer ist, der das Mobiltelefon aktiv und damit empfangsbereit schaltet. Als spezielle Garantie schützt das Fernmeldegeheimnis den telekommunikationsbezogenen Teilaspekt des Rechts auf informationelle Selbstbestimmung[134] und damit die Vertraulichkeit der Individualkommunikation. Geschützt werden also vorwiegend Kommunikationsinhalte. Die Kommunizierenden sollen so gestellt werden, als würden sie ohne fernmeldetechnische Mittel kommunizieren. Die näheren Umstände des Fernmeldevorgangs bzw. der Kommunikation werden aufgrund dieser Schutzrichtung nur insoweit von Art. 10 Abs. 1 GG erfasst, als sie überhaupt auf Kommunikationsinhalte beziehbar sind bzw. auf diese schließen lassen.[135] Rein technische Daten oder Details, die keine Rückschlüsse auf derartige Inhalte zulassen, sind daher vom Schutzbereich ausgenommen. IMSI- und IMEI-Kennungen stellen solche technischen Daten dar. Sie ermöglichen im Gegensatz zu Kommunikationsumständen keinen Rückschluss auf Kommunikationsinhalte oder –beziehungen.[136] Vielmehr ermöglichen sie beispielsweise, über regelmäßige Positionsmeldungen im Stand-by-Modus des Mobilfunkendgeräts dessen Position und damit den Standort einer Person zu ermitteln. Es handelt sich bei den Kennungen und gesendeten Standortdaten nicht um kommunikationsbezogene Daten.[137] Der Schutzzweck des Fernmeldegeheimnisses, nämlich die Gewährleistung der Vertraulichkeit von Kommunikation, wird durch die Übertragung der IMSI/IMEI-Kennungen gerade nicht berührt. Hinzu kommt, dass im Fall der Standortermittlung die Positionsmeldung des

Mobiltelefons vom Nutzer nicht einmal unmittelbar veranlasst wird; sie wird von ihm weder bemerkt, noch ist sie kontrollierbar.

Insgesamt bleibt damit festzuhalten, dass die vom IMSI-Catcher erfassten Daten nicht anlässlich eines Kommunikationsvorgangs anfallen. Der Datenaustausch erfolgt ausschließlich zur Herstellung und Sicherung der Betriebsbereitschaft des Mobiltelefons. Dieser Bereitschaftszustand ist erste technische Voraussetzung eines Kommunikationsvorgangs, nicht aber bereits ein Kommunikationsvorgang selbst.[138] Es fehlt also an dem für Art. 10 Abs. 1 GG erforderlichen Merkmal der Kommunikation.[139]

cc) Zusammenfassung

Die Erfassung der Geräte- und Kartennummer eines Mobiltelefons sowie der dazugehörigen Standortdaten unterfällt demnach nicht dem Schutzbereich des Fernmeldegeheimnisses.[140]

b) Recht auf informationelle Selbstbestimmung

aa) Grundsätzliches

Es könnte jedoch das Recht auf informationelle Selbstbestimmung betroffen sein. Dieses stellt eine Ausprägung des allgemeinen Persönlichkeitsrechts dar.[141] Abgeleitet wird diese Rechtsposition aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[142] Das Recht auf informationelle Selbstbestimmung gewährleistet dem Einzelnen die Befugnis, grundsätzlich selbst darüber zu entscheiden, ob und innerhalb welcher Grenzen persönliche Lebenssachverhalte und Daten erhoben, gespeichert, verwendet oder weitergegeben werden.[143] Hierdurch soll insbesondere vermieden werden, dass es aus Angst vor staatlichem Zugriff auf Daten zu einem Verzicht der Grundrechtsträger auf grundrechtlich geschützte Freiheiten und damit zu einem Einschüchterungseffekt kommt.[144] Der Grund für die besondere Schutzbedürftigkeit liegt dabei jedoch nicht allein in den Möglichkeiten der automatischen Datenerhebung und -verarbeitung. Vielmehr schützt das Recht auf informationelle Selbstbestimmung generell vor staatlicher Erhebung und Verarbeitung personenbezogener Daten, weil ihm als besondere Ausprägung des allgemeinen Persönlichkeitsrechts der Gedanke der Selbstbestimmung des Einzelnen immanent ist.[145] Geschützt werden jedoch nur personenbezogene Daten,[146] also solche zu persönlichen oder sachlichen Verhältnissen einer bestimmten Person (vgl. auch § 3 Abs. 1 BDSG). Hierzu zählen auch individualisierbare Daten. Denn unabhängig von der Sphäre, aus der die Daten stammen, sind diese sensibel und schutzbedürftig.[147]

bb) Ermittlung der IMSI/IMEI und der Standortdaten

IMSI und IMEI stellen solche personenbezogenen Daten dar.[148] Sie ermöglichen in mobilen Telekommunikationsnetzen die Identifizierung des Nutzers bzw. des benutzten Endgeräts durch den Netzbetreiber. Bei diesem sind die sog. Bestandsdaten i. S. des § 3 Nr. 3 TKG gespeichert. Diese beinhalten u.a. Angaben zur Person wie Name, Adresse und Geburtsdatum.[149] Die Bestandsdaten sowie die Rufnummer des Teilnehmers können bei Bedarf und bei Kenntnis der IMSI- oder IMEI-Kennung durch die zuständigen Behörden nach §§ 95, 113 TKG erfragt werden. Es handelt sich bei den Kennungen folglich um individualisierbare, personenbeziehbare Daten, also um solche Daten, die einen Schluss darauf zulassen, welche Person sich im Bereich der fingierten Funkzelle aufhält, und die es ermöglichen, weitere Daten über persönliche und sachliche Verhältnisse der Person zu erlangen. Darüber hinaus stellt auch die Standortermittlung mittels IMSI-Catcher eine Erhebung personenbezogener Daten dar. Damit kann der Aufenthaltsort des Mobilfunknutzers bestimmt werden. Zudem kann mittel- oder längerfristig auch ein Bewegungsprofil erstellt werden, das sodann Rückschlüsse auf das Verhalten der Person ermöglicht.

cc) Zusammenfassung

Der Einsatz des IMSI-Catchers führt in allen gesetzlich zulässigen Einsatzvarianten zur zielgerichteten Erhebung von individualisierbaren und damit personenbezogenen Daten. Der Schutzbereich des Grundrechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist demnach betroffen.

c) Meinungsfreiheit

Der Einsatz eines IMSI-Catchers führt grundsätzlich auch dazu, dass innerhalb seines Wirkbereichs für einen bestimmten Zeitraum Telekommunikation mittels Mobilfunkgeräten nicht möglich ist. Das Verhindern von Telekommunikation könnte eine Beeinträchtigung der grundrechtlich geschützten Freiheit auf Meinungsäußerung nach Art. 5 Abs. 1 S. 1 Hs. 1 GG darstellen. Dieses Freiheitsgrundecht schützt das Äußern und das Verbreiten von Meinungen sowie die Modalitäten der Verbreitung.[150] Auf das hierzu konkret gewählte Medium kommt es dabei nicht an.[151] Die Verbreitung kann daher auch mittels elektromagnetischer Wellen,[152] also auch mittels Mobiltelefon, erfolgen. Sofern der IMSI-Catcher eine Telekommunikation via Mobilfunk verhindert, nimmt er den Teilnehmern die Möglichkeit, einen bestimmten Adressatenkreis ungestört mit dem gewünschten Kommunikationsinhalt erreichen zu können.[153] Hierin liegt eine mittelbar-faktische Behinderung der Möglichkeit der Meinungsäußerung nach Art. 5 Abs. 1 S. 1 Hs. 1 GG.[154] Um jedoch einen grundrechtsrelevanten Eingriff darzustellen, muss diese faktische Einwirkung von einem solchen Gewicht, also einer solchen Schwere sein, dass sie einem gezielten, rechtlich regelnden Eingriff gleichzustellen ist.[155] Vorliegend wird die Möglichkeit der mobilen Telekommunikation für ein paar Sekunden, maximal für wenige Minuten, genommen. Die Beeinträchtigung ist von derart geringer Dauer, dass sie unter der Erheblichkeitsgrenze liegt und folglich die Schwelle zum Grundrechtseingriff nicht erreicht.[156] Zudem kann sich der Betroffene für die Zeit jedes anderen Mediums bedienen, um seine Meinung zu äußern oder zu verbreiten. Ein Eingriff in den Schutzbereich des Art. 5 Abs. 1 S. 1 GG liegt demnach nicht vor.

d) Allgemeine Handlungsfreiheit

Zu denken ist aber insofern an die allgemeine Handlungsfreiheit des Art. 2 Abs. 1 GG. Danach wird jedes menschliche Verhalten vor staatlichen Eingriffen und ohne Rücksicht darauf geschützt, welches Gewicht der Betätigung für die Persönlichkeitsentfaltung zukommt.[157] Hierzu zählt selbstverständlich auch die Möglichkeit, Telekommunikation zu betreiben. Soweit der IMSI-Catcher nun funktionsbedingt für einen kurzen Zeitraum die Herstellung einer Mobilfunkverbindung für ein einzelnes Mobiltelefon unmöglich macht und damit Telekommunikation unterbindet, ist das Grundrecht der allgemeinen Handlungsfreiheit betroffen.[158]

e) Zusammenfassung

Im Ergebnis ist demnach sowohl das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG als auch die allgemeine Handlungsfreiheit nach Art. 2 Abs. 1 GG betroffen.[159]

2. Verfassungsrechtliche Rechtfertigung

Der Einsatz des IMSI-Catchers führt zu einer Beeinträchtigung dieser Grundrechtspositionen[160] und müsste den Anforderungen an eine verfassungsrechtliche Rechtfertigung genügen. Die Befugnisnorm des § 100i StPO in ihrer seit 1. Januar 2008 geltenden Neufassung ist im Hinblick auf ihre Verfassungskonformität nicht unumstritten.

a) Gesetzesvorbehalt

Verfassungsrechtlich gerechtfertigte Eingriffe in das Recht auf informationelle Selbstbestimmung sowie in die allgemeine Handlungsfreiheit setzen zunächst voraus, dass sie auf einer gesetzlichen Grundlage beruhen,[161] die der Schrankentrias des Art. 2 Abs. 1 GG gerecht wird. Danach müsste der Gesetzesvorbehalt in Form der Rechte anderer, der verfassungsmäßigen Ordnung oder der Sittengesetze formell und materiell verfassungsgemäß ausgefüllt worden sein. Überragende Bedeutung kommt dabei der Schranke der *verfassungsmäßigen Ordnung* zu. Hierzu zählt die Gesamtheit der formell und materiell verfassungsmäßigen Normen.[162] Daneben kommt dem *Sittengesetz* ebenso wenig wie den *Rechten anderer* eine eigenständige Bedeutung bei der Grundrechtsbegrenzung zu.[163] Die Vorschrift des § 100i StPO – kompetenzgerecht und verfahrensfehlerfrei zustande gekommenes förmliches Gesetz – genügt dem Gesetzesvorbehalt in formeller Hinsicht.[164]

b) Zitiergebot

Auch ein Verstoß gegen das (formelle) Erfordernis des Zitiergebots liegt nicht vor. Bei Eingriffen in grundrechtlich geschützte Freiheiten gilt es regelmäßig, die in Art. 19 Abs. 1 S. 2 GG normierte Zitierpflicht zu beachten. Diese hat in erster Linie eine Warn- und Besinnungsfunktion, die den Gesetzgeber an seine Grundrechtsbindung erinnern soll und ihm die Folgen seiner Regelung im Hinblick auf Grundrechtseinschränkungen bewusst macht.[165] Sie verlangt, dass das betreffende Gesetz das davon beeinträchtigte Grundrecht unter Angabe des Artikels nennt und hierdurch ausdrücklich auf die Grundrechtseinschränkung hinweist.[166] Das Zitiergebot ist keine bloße Ordnungsvorschrift; ein Verstoß dagegen führt zur (Teil-)Nichtigkeit des einschränkenden Gesetzes.[167] In der Literatur wurde im Vorfeld der Entscheidung des BVerfG über die Vereinbarkeit von § 100i StPO a.F. mit dem Grundgesetz vielfach ein Verstoß gegen das Zitiergebot diskutiert.[168] Ein gesetzlicher Verweis auf die Einschränkung des Art. 10 Abs. 1 GG fehlte nämlich. Wie jedoch oben bereits dargelegt, ist der Schutzbereich des Art. 10 Abs. 1 GG nicht berührt, so dass eine diesbezügliche Zitierung nicht erforderlich ist. Und so hat der Gesetzgeber bei der Neufassung des § 100i StPO – im Anschluss an die Entscheidung des BVerfG – erneut zu Recht auf einen Hinweis auf Art. 10 GG verzichtet.[169] Einschlägig sind nur die durch Art. 2 Abs. 1 GG bzw. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG geschützten Grundrechte. Auf die Schrankenregelung des Art. 2 Abs. 1 GG findet das Zitiergebot aufgrund dessen restriktiver Auslegung jedoch keine Anwendung.[170] Die Grundrechte des Art. 2 Abs. 1 GG werden von vornherein nur unter dem Vorbehalt der verfassungsmäßigen Ordnung gewährleistet.[171] Ein Verstoß gegen das Zitiergebot liegt demnach entgegen einiger Stimmen in der Literatur nicht vor.[172]

c) Bestimmtheitsgrundsatz

Die Norm muss darüber hinaus dem aus dem Rechtsstaatsprinzip (vgl. Art. 20 Abs. 3 GG) abgeleiteten Bestimmtheitsgrundsatz, also dem Gebot der Normenklarheit und Widerspruchsfreiheit, Rechnung tragen.[173] Der Normbetroffene muss die Rechtslage erkennen und sein Verhalten darauf einrichten können.[174] Bezüglich des Rechts auf informationelle Selbstbestimmung erfordert dies, dass sowohl Anlass als auch Zweck und Grenzen des Eingriffs in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden.[175] Damit soll nicht nur sichergestellt werden, dass die bestehende Rechtsordnung dem Einzelnen eine verlässliche Grundlage für dessen Verhalten ist. Er soll darauf vertrauen können, dass die Exekutive steuernde und begrenzende Handlungsmaßstäbe vorfindet, und die Gerichte eine Rechtskontrolle durchführen können.[176] Der Bürger muss erkennen können, unter welchen Voraussetzungen sein Verhalten mit dem Risiko einer Überwachung verbunden ist.[177]

Der Gesetzgeber verwendet in § 100i Abs. 1 StPO den

Begriff der *Straftat von erheblicher Bedeutung* und damit einen unbestimmten Rechtsbegriff. Die Verwendung unbestimmter, auslegungsbedürftiger Rechtsbegriffe durch den Gesetzgeber steht dem Bestimmtheitsgebot jedoch grundsätzlich nicht entgegen,[178] sofern der Begriff bestimmbar ist und seine äußeren Grenzen derart abgesteckt sind, dass die Möglichkeit einer richterlichen Überprüfung besteht.[179] Kurzum, die Interpretationsbedürftigkeit eines Begriffs schließt folglich seine Bestimmtheit nicht per se aus.[180] Das Tatbestandsmerkmal der *Straftat von erheblicher Bedeutung* ist vom BVerfG und einigen Landesverfassungsgerichten gehalten und als hinreichend bestimmt erachtet worden.[181] Die nähere Konturierung und

Konkretisierung des Begriffs wurde der Rechtsprechung überantwortet.[182] Im Laufe der Zeit hat sich eine feststehende Definition herausgebildet. Danach liegt eine Straftat von erheblicher Bedeutung immer dann vor, wenn sie mindestens dem Bereich der mittleren Kriminalität zuzuordnen ist, den Rechtsfrieden empfindlich stört und dazu geeignet ist, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[183] Freilich wird sich jene Begriffskonkretisierung vorhalten lassen müssen, sie enthalte ihrerseits unbestimmte Rechtsbegriffe.[184] Daher wird teilweise eine restriktivere Auslegung des Tatbestandsmerkmals eingefordert.[185]

Betrachtet man den Begriff der *Straftat von erheblicher Bedeutung*, so ist es möglich, Konturen festzulegen und damit die äußeren Grenzen abzustecken. Während Bagatelldelikte, die nicht mindestens dem mittleren Kriminalitätsbereich zuzuordnen sind, ausscheiden, wird bei Verbrechen (vgl. § 12 StGB) in aller Regel die erhebliche Bedeutung zu bejahen sein.[186] Darüber hinaus hat der Gesetzgeber mit der Neufassung des § 100i StPO die Bedenken hinsichtlich der begrifflichen Unschärfe aufgegriffen und durch einen (nicht abschließenden) Verweis auf § 100a Abs. 2 StPO eine Konkretisierung des Begriffs vorgenommen. Das Vorliegen einer dort normierten Katalogtat ist als bedeutsamer Anwendungsfall des § 100i StPO hervorgehoben worden und daher ein wichtiger Anhaltspunkt für die rechtliche Bewertung des Begriffs der Straftat von erheblicher Bedeutung. Soweit über den Katalog des § 100a Abs. 2 StPO hinaus Straftaten den für Maßnahmen nach § 100i StPO erforderlichen Erheblichkeitsgrad erreichen können, ist dies unschädlich. Es ist dem Gesetzgeber nicht immer möglich, abschließende Straftatenkataloge zu normieren. So wird es etwa im Bereich der Vergehen häufig an der notwendigen erheblichen Bedeutung mangeln. Andererseits können die Taten auch hier im Einzelfall schwer wiegen und ein Vorgehen nach § 100i StPO erforderlich machen. Wann dies konkret der Fall ist, ist ausgehend von der Begriffskonkretisierung der Rechtsprechung und mit vergleichendem Blick auf die Schwere der in § 100a Abs. 2 StPO genannten Katalogtaten sowie unter Berücksichtigung der Umstände des Einzelfalles zu ermitteln. Diese Subsumtion durch die Strafverfolgungsbehörden ist justitiabel. Und auch die Einzelfallprüfung darf freilich nicht nach willkürlichen Maßstäben erfolgen, sondern muss sich nach Ausmaß des Schadens, der Art und Gefährlichkeit der Tatbegehung und Bedrohung der Allgemeinheit richten.[187]

Im Ergebnis handelt es sich bei dem Begriff *der Straftat von erheblicher Bedeutung* um einen bestimmbaren Rechtsbegriff, der dem verfassungsrechtlichen Bestimmtheitsgebot genügt.[188]

d) Grundsatz der Verhältnismäßigkeit

Schließlich muss die gesetzliche Regelung zum Einsatz des IMSI-Catchers den Anforderungen des Grundsatzes der Verhältnismäßigkeit entsprechen. Dieser wird unmittelbar aus dem Rechtsstaatsprinzip abgeleitet[189] und umfasst die drei Teilgebote der Geeignetheit, Erforderlichkeit und Angemessenheit staatlicher Maßnahmen.[190]

aa) Legitimer Zweck

Bezugspunkt der drei Kriterien der Verhältnismäßigkeitsprüfung ist der mit der Einschränkung der Grundrechte verfolgte Zweck. Dieser muss vor der Rechtsordnung und insbesondere dem Grundgesetz Bestand haben;[191] der Zweck muss also verfassungslegitim sein.[192] Mit der Regelung in § 100i StPO wollte der Gesetzgeber die Voraussetzungen für eine effektive Strafverfolgung, insbesondere im Bereich der organisierten Kriminalität, schaffen.[193] Die Ermittlung der IMSI-/IMEI-Kennungen oder des Standorts eines Mobiltelefons sind zur Vorbereitung weiterer strafprozessualer Maßnahmen oftmals unerlässlich. Die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der etwaige Freispruch des Unschuldigen stellen wesentliche Aufgaben der Strafrechtspflege dar. Letztere soll den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren durchsetzen.[194] Die Schaffung entsprechender strafprozessualer Normen sowie deren Anwendung dienen der Aufrechterhaltung einer

funktionstüchtigen Strafrechtspflege und damit einem Gut von Verfassungsrang.[195] Ein legitimer Zweck ist demnach gegeben.

bb) Geeignetheit

Der durch § 100i StPO mögliche Einsatz des IMSI-Catchers müsste zur Erreichung dieses Zwecks geeignet sein. Dies ist der Fall, wenn sich mit der Maßnahme die Wahrscheinlichkeit erhöht, dass der angestrebte Erfolg eintritt, wenn also dadurch der gewünschte Erfolg gefördert werden kann.[196] Da dem Gesetzgeber auf der Stufe der Eignung einer Maßnahme eine weit reichende Einschätzungsprärogative zukommt, genügt schon die abstrakte Möglichkeit der Zweckerreichung.[197] Der IMSI-Catcher ist in der Lage, unbekannte Geräte- und SIM-Kartenkennungen festzustellen. Er ermöglicht damit die Ermittlung der Rufnummer des Beschuldigten als notwendige Voraussetzung für weitere Ermittlungsmaßnahmen, insbesondere die Anordnung und Durchführung einer Telekommunikationsüberwachung.[198] Darüber hinaus erlaubt der Einsatz des IMSI-Catchers den Strafverfolgungsbehörden die Feststellung des Standorts eines gesuchten Mobilfunkgeräts und damit des möglichen Aufenthaltsorts eines Beschuldigten. Der IMSI-Catcher fördert also die Aufklärung und Verfolgung von Straftaten und trägt damit zum Funktionieren der Strafrechtspflege bei. Dessen Geeignetheit ist zu bejahen.

cc) Erforderlichkeit

Der Einsatz des IMSI-Catchers müsste auch erforderlich sein. Die Erforderlichkeit einer staatlichen Maßnahme steht immer dann in Frage, wenn ein milderes Mittel zur Verfügung steht, das in gleicher Weise geeignet ist, den angestrebten Zweck zu erreichen.[199] Maßnahmen nach § 100i StPO dienen regelmäßig der Vorbereitung weiterer strafprozessualer Zwangsmaßnahmen.

Zu erwägen wäre hier ein Rückgriff auf weniger eingriffsintensive klassische Ermittlungsmethoden wie die Zeugenbefragung, die Observation oder die Anfrage beim Telekommunikationsanbieter nach §§ 112, 113 TKG. Dabei ist allerdings zu berücksichtigen,

dass sich der dem Gesetzgeber auf der Stufe der Geeignetheit zugestandene Beurteilungs- und Prognosespielraum auch auf die Prüfung der Erforderlichkeit auswirkt. Denn das Erfordernis des geringstmöglichen Eingriffs gilt nur im Verhältnis gleichermaßen geeigneter Maßnahmen.[200] Im Bereich der Bekämpfung der organisierten Kriminalität, die der Gesetzgeber bei der Legalisierung des Einsatzes des IMSI-Catchers im Auge gehabt hat, sind die weniger eingriffsintensiven herkömmlichen Ermittlungsmethoden aber nicht als gleich geeignet anzusehen. Sie reichen zur Bekämpfung der organisierten Kriminalität, welche sich durch eine besondere Qualität der Organisation und schnelle Anpassung ihrer Strukturen auszeichnet, nicht aus und wären überdies deutlich aufwändiger.

Hinsichtlich der Standortbestimmung könnte als milderes Mittel eine Ortung via GPS oder *stiller SMS* in Betracht zu ziehen sein. Eine Ortung von Mobiltelefonen mittels GPS ist jedoch mit einem enormen technischen und auch finanziellen Aufwand verbunden. Hinzu kommt, dass in Deutschland Mobilfunkgeräte mit GPS-Chip deutlich weniger verbreitet sind als etwa in den USA.[201] Straftäter dürften sich zudem in der Regel Mobilfunkgeräte ohne GPS-Empfänger anschaffen. Eine Ortung via GPS ist daher nicht gleich geeignet. Gezweifelt werden muss darüber hinaus auch daran, dass es sich bei der GPS-Ortung tatsächlich um ein milderes Mittel handelt. Zwar kommt es hierbei nicht zu einer Erhebung von personenbezogenen Daten einer Vielzahl von Personen. Für den Betroffenen dürfte aber die damit mögliche automatische Erstellung eines kompletten Bewegungsbildes schwerer wiegen.[202] Die *stille SMS* dagegen funktioniert dergestalt, dass sie ein Signal an ein bekanntes Mobilfunkgerät sendet und so beim Mobilfunkanbieter Verbindungsdaten erzeugt, denen u.a. entnommen werden kann, in welcher Mobilfunkzelle das Mobiltelefon gerade eingebucht ist. Der Vorteil der *stillen SMS* ist ihr einfacher, zeitsparender Einsatz. Zudem ist nicht erforderlich, dass sich die Ermittler in der Nähe der gesuchten Person aufhalten.[203] Andererseits ist eine exakte Feststellung des Aufenthaltsorts des Beschuldigten, wie sie der IMSI-Catcher zulässt, indem er (kleinere) Funkzellen fingiert, häufig nicht möglich. Die Funkzellen divergieren in ihrer Reichweite erheblich und können größere Ausmaße annehmen.[204] Berücksichtigt man die dem Gesetzgeber zugestandene Einschätzungsprärogative, so ist der Einsatz des IMSI-Catchers nach § 100i StPO als erforderlich anzusehen.

dd) Angemessenheit

Zuletzt muss der Einsatz des IMSI-Catchers nach § 100i StPO auch angemessen, also verhältnismäßig im engeren Sinne, sein. Die durch ihn verursachten Beeinträchtigungen dürfen nicht außer Verhältnis zu dem Gewicht und der Dringlichkeit der durch die Maßnahme geförderten Gemeinwohlbelange stehen.[205] Die besondere Beeinträchtigung besteht vorliegend darin, dass durch den Einsatz des IMSI-Catchers nicht nur, wie sonst bei Zwangsmaßnahmen üblich, in die Grundrechte des Beschuldigten eingegriffen wird, sondern gleichzeitig eine Vielzahl unbeteiligter Dritter betroffen ist. Der Eingriff entfaltet also eine sehr große Streubreite und ist aufgrund der Vielzahl der betroffenen Grundrechtsträger von besonde-

rer quantitativer Intensität.[206] Ein Eingriff von derart quantitativ hoher Intensität kann nur im Interesse hochrangiger Rechtsgüter,[207] namentlich den besonderen Belangen der Allgemeinheit, gerechtfertigt werden.

Ein solches qualifiziertes Rechtsgut stellt das gleichfalls Verfassungsrang genießende Gebot der Aufrechterhaltung einer funktionstüchtigen Strafrechtspflege dar.[208] Die vermehrte Nutzung moderner Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche hat die Strafverfolgung erschwert, weil es im Zuge dieser Entwicklung eben auch zu einer Effektivierung krimineller Vorgehensweisen kommt.[209] Gerade im Bereich der Telekommunikationsüberwachung fällt es den Beschuldigten besonders leicht, sich durch Austausch von Mobilfunkgeräten oder SIM-Karten der Überwachung durch die Strafverfolgungsbehörden zu entziehen. Dies geschieht umso häufiger im Bereich der organisierten Kriminalität. Im Sinne und Interesse einer effektiven Strafverfolgung, die zu den unverzichtbaren Verfassungsaufgaben des Staates zählt,[210] hat der Gesetzgeber auf technische Entwicklungen zu reagieren. Dabei handelt es sich nicht lediglich um eine sinnvolle Abrundung des Arsenals kriminalistischer Ermittlungsmethoden, die weiterhin wirkungsvolle herkömmliche Ermittlungsmaßnahmen ergänzt.[211] Es geht vielmehr darum, gegenzusteuern und zu verhindern, dass sich Schlupflöcher auftun, durch die sich Schwer- und Schwerstkriminelle den Strafverfolgungsbehörden entziehen. Der Gesetzgeber hat mit dem in § 100i StPO verankerten Merkmal der Straftat von erheblicher Bedeutung einer exzessiven Verwendung des IMSI-Catchers einen Riegel vorgeschoben.

In qualitativer Hinsicht ist der Eingriff in die Rechte unbeteiligter Dritter eher als minder schwerwiegend anzusehen.[212] § 100i Abs. 2 StPO enthält verfahrensmäßige Vorschriften über die Verwendung von Daten Unbeteiligter. Eine Deanonymisierung der ermittelten Kennungen findet nicht statt. Im Gegenteil, eine Benachrichtigung mitbetroffener Dritter, die voraussetzen würde, dass die IMSI-/IMEI-Kennungen mit Hilfe der Netzbetreibers einer Person zugeordnet werden, würde den Grundrechtseingriff noch erheblich vertiefen.[213] Gesetzlich vorgesehene Sicherungen, wie Kennzeichnungs- und Löschungspflichten sowie ein absolutes Verwendungsverbot bezüglich der Daten (vgl. § 100i Abs. 2 S. 2 StPO), sorgen dafür, dass die Eingriffsintensität für den einzelnen unbeteiligten Dritten als eher gering anzusehen ist.

Im Ergebnis ist festzuhalten, dass die mit dem Einsatz des IMSI-Catchers verbundene Grundrechtsbeeinträchtigung in keinem Missverhältnis zu dem mit der Maßnahme verfolgten Zweck steht. Durch besondere Schutzmechanismen hat der Gesetzgeber dem Umstand, dass die Maßnahme eine große Streubreite aufweist, hinreichend Rechnung getragen. Auch darüber hinausgehende kurzfristige Störungen, die bei den Netzbetreibern oder Mobilfunkteilnehmern während des Einsatzes auftreten können, und deren Rechtfertigung an Art. 2 Abs. 1 GG zu messen ist, sind aufgrund der Geringfügigkeit der Störung und gemessen an den Bedürfnissen der Strafrechtspflege hinzunehmen.[214] Zudem ist in Rechnung zu stellen, dass von der Befugnis nach § 100i StPO nur in geringem Umfang Gebrauch gemacht wird.[215] § 100i StPO ist demnach auch als verhältnismäßig im engeren Sinne anzusehen.

3. Ergebnis

Der nach § 100i StPO mögliche Einsatz des IMSI-Catchers stellt damit keinen Verstoß gegen die in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie Art. 2 Abs. 1 GG geschützten Grundrechtspositionen dar.

V. Schlussbetrachtung

Zusammenfassend lässt sich sagen, dass der Gesetzgeber mit der Schaffung und Neufassung des § 100i StPO die Möglichkeiten der strafprozessualen Datenerhebung erweitert hat und damit freilich dem Ausgangszitat Futter gibt. Die Befugnisnorm stellt sich jedoch als verfassungsgemäß dar. Insbesondere entspricht sie dem Verhältnismäßigkeitsgrundsatz. Die Anwendung der Vorschrift durch die Strafverfolgungsbehörden wird jedoch zeigen, inwieweit den verfassungsrechtlichen Anforderungen auch im Einzelfall Rechnung getragen wird. Von zentraler Bedeutung – und daher besonders anzumahnen – ist dabei der sensible Umgang mit erhobenen Daten unbeteiligter Personen. Zudem ist denkbar, dass die Zukunft die Entwicklung technischer Neuerungen mit sich bringt, mit deren Hilfe mindestens gleich wirksam, aber noch milder im Hinblick auf die Grundrechte unbeteiligter Dritter vorgegangen werden kann.

---

* Ref. iur. Stefanie Harnisch ist Doktorandin am Lehrstuhl für Strafrecht, Strafprozessrecht und europäisches Strafrecht an der Juristenfakultät Leipzig. Ref. iur. Martin Pohlmann ist Doktorand am Lehrstuhl für Bürgerliches Recht, Arbeits- und Sozialrecht an der Juristenfakultät Leipzig.

[1] *Heribert Prantl*, SZ vom 2. Juli 2007, Nr. 149, S. 4.

[2] Vgl. BVerfG NVwZ 2009, 96 = HRRS 2008 Nr. 1005.

[3] Gesetz zur Änderung der StPO, BGBl. I 2002, S. 3018 f.

[4] Vgl. *Bär* MMR 2003, VI, VIII; *Fox* DuD 2002, 212.

[5] Der Begriff des *IMSI-Catchers* wird im Gesetzestext als solcher nicht verwendet. In der entsprechenden Regelung ist von technischen Mitteln die Rede. Das einzige technische Mittel, das die vom Gesetz vorgesehenen Maßnahmen ohne weitere Schritte und Hilfsmittel erfüllt, ist der IMSI-Catcher. Zudem hatte der Gesetzgeber bei Schaffung des § 100i StPO einzig und allein den IMSI-Catcher im Auge. Vgl. *Bär* MMR 2003, VI; *Eisenberg/Singelnstein* NStZ 2005, 62, 63 f.; *Hilger* GA 2002, 557 f.

[6] *Bär* MMR 2003, VI; *Fox* DuD 2002, 212, 213; *Hilger* GA 2002, 557; *Keller*, Die Ermittlung der Kennungen und des Standorts von Mobilfunkgeräten im Spannungsfeld zwischen Kriminalitätsbekämpfung und Verfassungsmäßigkeit (2008), S. 40.

[7] Heghmanns/Scheffler/*Murmann*, Handbuch zum Strafverfahren (2008), III Rn. 241; Löwe-Rosenberg/ *Schäfer* , StPO, 25. Aufl. (2004), § 100i Rn. 3.

[8] *Fox* DuD 2002, 212, 213; SK-StPO/*Wolter*, Losebl., Stand: 59. Lfg. (Okt. 2008), § 100i Rn. 21.

[9] Heghmanns/Scheffler/*Murmann*, a.a.O. (Fn. 7), III Rn. 241.

[10] *Keller*, a.a.O. (Fn. 6), S. 41; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100a Rn. 16, § 100i Rn. 3.

[11] *Bär* MMR 2003, VI, VII; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 3.

[12] Heghmanns/Scheffler/*Murmann*, a.a.O. (Fn. 7), III Rn. 225; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 3.

[13] *Artkämper* Kriminalistik 1998, 202, 207 (Fn. 4); SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 20.

[14] Vgl. Legaldefinition nach § 4 Nr. 5 TKÜV a.F.; *Artkämper* Kriminalistik 1998, 202.

[15] *Eisenberg/Singelnstein* NStZ 2005, 62 (Fn. 2).

[16] *Keller*, a.a.O. (Fn. 6), S. 42; *Löffelmann* AnwBl. 2006, 598, 600; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 3; Vordermayer/Heintschel-Heinegg/*Mayer*, Hdb. für den Staatsanwalt, 3. Aufl. (2008), 1. Teil, 1. Kap., Rn. 70.

[17] Der Funkkontakt zu der jeweiligen Basisstation wird hierbei ca. alle 2, 4 Sekunden erneuert; *Gercke* CILIP 2002, 20, 22; *Welp* NStZ 1994, 209, 210 (Fn. 14).

[18] *Keller*, a.a.O. (Fn. 6), S. 42; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 3.

[19] *Gercke*, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren (2002), S. 30; *Löffelmann* AnwBl. 2006, 598, 600.

[20] *Gercke* CILIP 2002, 20, 22; *Hilger* GA 2002, 557.

[21] *Gercke* CILIP 2002, 20, 26; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 3.

[22] *Roggan* KritV 2003, 76, 87; Vordermayer/Heintschel-Heinegg/*Mayer*, a.a.O. (Fn. 16), 1. Teil, 1. Kap., Rn. 70.

[23] *Fox* DuD 2002, 212; *ders.* DuD 1997, 539; Löwe-Rosenberg/ *Schäfer* , a.a.O. (Fn. 7), § 100i Rn. 1.

[24] *Denkowski* Kriminalistik 2002, 117; *Fox* DuD 2002, 212, 214; *Keller*, a.a.O. (Fn. 6), S. 43.

[25] Vordermayer/Heintschel-Heinegg/*Mayer*, a.a.O. (Fn. 16), 1. Teil, 1. Kap., Rn. 70.

[26] *Eisenberg/Singelnstein* NStZ 2005, 62 (Fn. 2); *Keller*, a.a.O. (Fn. 6), S. 46.

[27] Durch diese verstärkte Sendeleistung ist die virtuelle Funkzelle jedoch wesentlich kleiner als eine reguläre Zelle, vgl. SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 21.

[28] *Keller*, a.a.O. (Fn. 6), S. 46; KK/*Nack*, StPO, 6. Aufl. (2008), § 100i Rn. 5; *Roggan* KritV 2003, 76, 86.

[29] *Gercke* MMR 2003, 453, 454; *Löwnau-Iqbal* DuD 2001, 578.

[30] *Günther* NStZ 2005, 485, 486 (Fn. 14).

[31] Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100a Rn. 16.

[32] *Bär* MMR 2003, VI, VII; *Fox* DuD 2002, 212, 213.

[33] *Deckers* StraFo 2002, 109, 112; *Keller*, a.a.O. (Fn. 6), S. 40.

[34] *Fox* DuD 2002, 212, 213; *Gercke*, a.a.O. (Fn. 19), S. 30.

[35] *Gercke* StraFo 2003, 76, 78.

[36] *Gercke* CILIP 2002, 20, 22; *Keller*, a.a.O. (Fn. 6), S. 79.

[37] *Eckhardt* CR 2002, 770, 771; *Gercke* StraFo 2003, 76, 78.

[38] *Keller*, a.a.O. (Fn. 6), S. 50; *Roggan* KritV 2003, 76, 86.

[39] *Bär* MMR 2003, VI, VII; *Fox* DuD 2002, 212, 214; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 4.

[40] Zur Praxistauglichkeit des IMSI-Catchers unter III 3.

[41] Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 4; *Roggan* KritV 2003, 76, 86.

[42] *Gercke* StraFo 2003, 76, 78; *Keller*, a.a.O. (Fn. 6), S. 50.

[43] *Fox* DuD 2002, 212, 214.

[44] *Keller*, a.a.O. (Fn. 6), S. 50; *Roggan* KritV 2003, 76, 86.

[45] *Fox* DuD 2002, 212, 214; *Keller*, a.a.O. (Fn. 6), S. 50. – Die Überwachung und Aufzeichnung von Kommunikationsinhalten mittels IMSI-Catcher ist sowohl nach § 100i StPO a.F. als auch nach der Neuregelung nicht zulässig.

[46] *Keller*, a.a.O. (Fn. 6), S. 52; *Roggan* KritV 2003, 76, 86.

[47] *Fox* DuD 2002, 212, 214 f.; *Keller*, a.a.O. (Fn. 6), S. 52.

[48] BT-Drs. 14/6885, S. 4; Krekeler/Löffelmann/*Löffelmann*, StPO, 1. Aufl. (2007), § 100i Rn. 2.

[49] *Fox* DuD 2002, 212, 215.

[50] *Deckers* StraFo 2002, 109, 112; Vordermayer/Heintschel-Heinegg/*Mayer*, a.a.O. (Fn. 16), 1. Teil, 1. Kap., Rn. 70.

[51] *Fox* DuD 1997, 539; *Keller*, a.a.O. (Fn. 6), S. 52 f.

[52] *Keller*, a.a.O. (Fn. 6), S. 53. – Die Bundesregierung sieht eine solche Gefahr als gering an, BT-Drs. 14/6885, S. 2.

[53] Eingeführt durch BGBl. I 2008, 3083 ff.

[54] BT-Drs. 14/6885, S.1.

[55] Vgl. *Bär* MMR 2003, VI, VIII; *Denkowski* Kriminalistik 2002, 117, 121.

[56] BGH Ermittlungsrichter CR 1998, 738; a.A. LG Hamburg NStZ-RR 1999, 82.

[57] *Denkowski* Kriminalistik 2002, 117, 122. – Ablehnend wegen Verstoßes gegen den Bestimmtheitsgrundsatz *Gercke* CILIP 2002, 20, 27.

[58] AG München, Beschluss vom 5. September 2001 (Gz. ER II Gs 9039/01), zitiert nach BR-Drs. 452/1/02, S. 3; vgl. auch BT-Drs. 14/9801, S. 9; *Bär* MMR 2003, VI, VIII.

[59] *Denkowski* Kriminalistik 2002, 117, 220. – Diese Ansicht griff der Bundesrat im Jahre 2002 im Rahmen eines Gesetzentwurfs auf und schlug eine Regelung durch Ergänzung des § 100c Abs. 1 Nr. 1 lit. b StPO a.F. vor. Er stützte sich dabei ausdrücklich auf die seiner Ansicht nach vorzugswürdige und von der Rechtsprechung bereits vertretene "vermittelnde Lösung" der Anwendung des § 100c Abs. 1 Nr. 1 lit. b StPO a.F. (vgl. BT-Drs. 14/9801, S. 9). Dieser Vorschlag wurde jedoch von Bundesregierung und Bundestag nicht gestützt. Ebenso hatte ein Antrag der Länder Hessen und Bayern vom 23. Februar 2004, der erneut die Änderung des § 100c Abs. 1 Nr. 1 lit. b StPO a.F. vorsah, keinen Erfolg (vgl. BR-Drs. 163/04, S. 12 f.).

[60] Gestützt auf eine Auskunft des BMI *Fox* DuD 2002, 212.

[61] *Bär* MMR 2003, VI, VIII; *Denkowski* Kriminalistik 2002, 117, 119. – Vgl. auch Der Spiegel, 13. August 2001, Heft 33/2001, 54, 55.

[62] Vgl. *Gercke* CILIP 2002, 20, 27; *ders.* MMR 2003, 453, 454; *Keller*, a.a.O. (Fn. 6), S. 54; *Löwnau-Iqbal* DuD 2001, 578; kritisch auch *Bär* MMR 2003, VI.

[63] BT-Drs. 13/8016 = BR-Drs. 369/97.

[64] Vgl. BR-Drs. 369/1/97, S. 4 = BT-Drs. 13/8453, S. 3.

[65] Vgl. BT-Drs. 14/850, S. 80; *Löwnau-Iqbal* DuD 2001, 578.

[66] Vgl. Der Spiegel, 13. August 2001, Heft 33/2001, 54 zum Einsatz des IMSI-Catchers durch Sicherheitsbehörden.

[67] BT-Drs. 14/7562.

[68] BT-Drs. 14/9088, S. 2, 4 ff.

[69] Vgl. BT-Drs. 14/9801, S. 14; BR-Drs. 452/02. – Vgl. auch *Keller*, a.a.O. (Fn. 6), S. 64.

[70] BGBl. I 2002, S. 3018.

[71] BGBl. I 2004, S. 2198, 2203; BGBl. I 2005, S. 1841, 1845.

[72] Vgl. zum Ganzen BT-Drs. 16/5846, S. 56. – Zur Kritik BR-Drs. 452/1/02; *Albrecht/Dorsch/Krüpe*, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation (2003), S. 204.

[73] BVerfGE 103, 21, 34. – Hierzu *Rieß* GA 2004, 623, 628 f.

[74] *Meyer-Goßner*, StPO, 51. Aufl. (2008), § 100i Rn. 8.

[75] Vgl. KK/*Nack*, a.a.O. (Fn. 28), § 100i Rn. 7, § 110a Rn. 21. – Ob es sich um eine Straftat von erheblicher Bedeutung handelt, ergibt sich allerdings vielfach erst im Laufe der Ermittlungen; *Meyer-Goßner*, a.a.O. (Fn. 74), § 98a Rn. 5.

[76] SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 26. – Vgl. auch *Bär* MMR 2003, VI, IX, der den Anwendungsbereich dieser Regelung folglich für sehr gering hielt.

[77] Diese musste trotz Nichterwähnung im Wortlaut auch im Einzelfall von erheblicher Bedeutung sein; vgl. Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100g Rn. 13.

[78] Der Untersuchungsgrundsatz umfasst die Pflicht, die materielle Wahrheit zu erforschen und den Sachverhalt aufzuklären, vgl. Krekeler/Löffelmann/*Löffelmann*, a.a.O. (Fn. 48), § 160 Rn. 2.

[79] BT-Drs. 16/5846, S. 56; *Bär* MMR 2008, 215, 221. – Vgl. zur vorherigen Rechtslage *Keller*, a.a.O. (Fn. 6), S. 85 f.; *Meyer-Goßner*, StPO, 50. Aufl. (2007), § 100i Rn. 6a.

[80] Vgl. *Hilger* GA 2002, 557, 558; *Keller*, a.a.O. (Fn. 6), S. 85.

[81] Vgl. KK/*Nack*, StPO, 5. Aufl. (2003), § 100i Rn. 8 sowie Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 13, die diese Variante für systemwidrig hielten. – A.A. *Meyer-Goßner*, a.a.O. (Fn. 79), § 100i Rn. 6.

[82] Das Gesetz sprach hier vom *Täter*, was der Systematik der StPO und dem Grundverständnis verfassungsrechtlicher Garantien im Strafverfahren (etwa Unschuldsvermutung) grundlegend widerspricht. – Vgl. auch *Roggan* KritV 2003, 76, 87; *Ruhmannseder* JA 2007, 47, 49.

[83] Der Einsatz des IMSI-Catchers zur Erforschung des Sachverhalts wird entgegen des weiter reichenden Wortlauts des § 100f Abs. 3 S. 2 StPO a.F. als nicht zulässig erachtet, vgl. *Keller*, a.a.O. (Fn. 6), S. 86. Ebenso zur vormaligen inhaltsgleichen Regelung des § 100c Abs. 2 S. 2 StPO a.F. SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 29. – Unzutreffend *Bär* MMR 2003, VI, IX.

[84] *Gercke* MMR 2003, 453, 455.

[85] SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 26.

[86] Diese einfache Subsidiaritätsklausel wurde teilweise als praxisfern und eher obsolet bezeichnet; *Hilger* GA 2002, 557, 559; SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 28.

[87] BT-Drs. 16/5846, S. 66; KK/*Nack*, a.a.O. (Fn. 28), § 100i Rn. 12; *Meyer-Goßner*, a.a.O. (Fn. 74), § 477 Rn. 5.

[88] Betrifft den Fall des sog. Nachrichtenmittlers i. S. des § 100a Abs. 3 StPO.

[89] BVerfG NJW 2007, 351, 354 ff. = HRRS 2006 Nr. 807; *Meyer-Goßner*, a.a.O. (Fn. 74), § 100i Rn. 14; *Roggan* KritV 2003, 76, 87, wonach die Vermeidbarkeit der Inanspruchnahme Dritter aufgrund der weiten Verbreitung von Mobiltelefonen theoretischer Natur ist.

[90] KK/*Nack*, a.a.O. (Fn. 28), § 100i Rn. 11 und *Löffelmann* AnwBl. 2006, 598, die deshalb in diesen Fällen einen Eingriff in die Rechte Dritter verneinen.

[91] Ein Verstoß gegen das in § 100i Abs. 2 S. 2 StPO normierte Verwendungsverbot begründet ein Verwertungsverbot; vgl. *Keller*, a.a.O. (Fn. 6), S. 131; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 40; in diesem Sinne auch *Joecks*, StPO, 2. Aufl. (2008), § 100i Rn. 8; *Ruhmannseder* JA 2007, 47, 49.

[92] *Meyer-Goßner*, a.a.O. (Fn. 74), § 100i Rn. 14; SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 33. – Kritisch jedoch BT-Drs. 14/7727, S. 6; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 14.

[93] KK/*Griesbaum*, a.a.O. (Fn. 28), § 160a Rn. 11; *Meyer-Goßner*, a.a.O. (Fn. 74), § 160a Rn. 7.

[94] Vgl. *Albrecht/Dorsch/Krüpe*, a.a.O. (Fn. 72), S. 199 ff., 208.

[95] *Fox* DuD 2002, 212, 214.

[96] *Günther* Kriminalistik 2004, 11, 12.

[97] Die IMEI-gestützte Telekommunikationsüberwachung war nach Auffassung des Gesetzgebers bereits nach der alten Rechtslage zulässig. Die gesetzliche Neuregelung dient insoweit lediglich der Klarstellung; BT-Drs. 16/5846, S. 26.

[98] Ausführlich hierzu *Eisenberg/Singelnstein* NStZ 2005, 62 ff. – Dieses Observationsmittel wird jedoch allgemein nicht als von § 100i StPO gedeckt angesehen; vgl. *Meyer-Goßner*, a.a.O. (Fn. 74), § 100i Rn. 4.

[99] BT-Drs. 15/5252, S. 93; *Keller*, a.a.O. (Fn. 6), S. 88.

[100] *Eisenberg/Singelnstein* NStZ 2005, 62.

[101] Nach BT-Drs. 15/5252, S. 93 soll eine Ortung auf bis zu 50 Meter genau erfolgen können.

[102] Damit soll der Standort auf bis zu 50 Meter genau bestimmt werden können; vgl. BGHSt 46, 266, 271.

[103] Vgl. *Bär* MMR 2003, VI, IX, der den IMSI-Catcher als ein aus kriminalistischer Sicht wichtiges Mittel bezeichnet.

[104] Vgl. auch Krekeler/Löffelmann/*Löffelmann*, a.a.O. (Fn. 48), § 100i Rn. 1, der die Anwendungshäufigkeit der Maßnahme aufgrund des damit verbundenen Aufwands dennoch als gering erachtet.

[105] *Bär* MMR 2008, 215, 221; *Meyer-Goßner*, a.a.O. (Fn. 74), § 100i Rn. 1; *Haller/Conzen*, Das Strafverfahren, 5. Aufl. (2008), Rn. 1038. – Fraglich *Joecks*, a.a.O. (Fn. 91), § 100i Rn. 1, wonach die Voraussetzungen im Wesentlichen gleich geblieben sind.

[106] *Hufen*, StaatsR II, 1. Aufl. (2007), § 17 Rn. 3; *Pieroth/Schlink*, GrundR, 24. Aufl. (2008), § 19 Rn. 762.

[107] Dreier/*Hermes*, GG, Band I, 2. Aufl. (2004), Art. 10 Rn. 36; v. Mangoldt/Klein/Starck/*Gusy*, GG, Band 1, 5. Aufl. (2005), Art. 10 Rn. 40; v. Münch/Kunig/*Löwer*, GG, Band 1, 5. Aufl. (2000), Art. 10 Rn. 18.

[108] St. Rspr. BVerfGE 115, 166, 183; 110, 33, 53; 100, 313, 359.

[109] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; *Gercke*, a.a.O. (Fn. 19), S. 66; *Gusy* Jus 1986, 89, 90.

[110] BVerfGE 46, 120, 143; *Ipsen*, StaatsR II, 11. Aufl. (2008), § 6 Rn. 306; *Keller*, a.a.O. (Fn. 6), S. 137.

[111] *Pieroth/Schlink*, a.a.O. (Fn. 106), § 19 Rn. 773; v. Münch/Kunig/*Löwer*, a.a.O. (Fn. 107), Art. 10 Rn. 12.

[112] BVerfGE 106, 28, 36; *Gercke*, a.a.O. (Fn. 19), S. 66; *Hufen*, a.a.O. (Fn. 106), § 17 Rn. 7; Jarass/Pieroth/*Jarass*, GG, 10. Aufl. (2009), Art. 10 Rn. 5.

[113] *Hufen*, a.a.O. (Fn. 106), § 17 Rn. 7; *Ipsen*, a.a.O. (Fn. 110), § 6 Rn. 306; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 10 Rn. 5; *Pieroth/Schlink*, a.a.O. (Fn. 106), § 19 Rn. 773; Sachs/*Pagenkopf*, GG, 5. Aufl. (2009), Art. 10 Rn. 14 f.

[114] V. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 42, 45.

[115] BVerfGE 110, 33, 52 f.; 107, 299, 312; *Gercke*, a.a.O. (Fn. 19), S. 67; v. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 45.

[116] St. Rspr. vgl. BVerfGE 115, 166, 183; 113, 348, 364; *Gercke*, a.a.O. (Fn. 19), S. 67; *Hufen*, a.a.O. (Fn. 106), § 17 Rn. 7.

[117] Sachs/*Pagenkopf*, a.a.O. (Fn. 113), Art. 10 Rn. 14; v. Münch/Kunig/*Löwer*, a.a.O. (Fn. 107), Art. 10 Rn. 22.

[118] BVerfGE 113, 348, 365; *Gercke*, a.a.O. (Fn. 19), S. 67; *Keller*, a.a.O. (Fn. 6), S. 139; *Nachbaur* NJW 2007, 335, 336 f.; Sachs/*Pagenkopf*, a.a.O. (Fn. 113), Art. 10 Rn. 14.

[119] BVerfG NJW 2007, 351 ff. = HRRS 2006 Nr. 807.

[120] Vgl. auch *Nachbaur* NJW 2007, 335.

[121] BVerfGE 113, 348, 364; 100, 313, 358; *Hufen*, a.a.O. (Fn. 106), § 17 Rn. 10; v. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 103.

[122] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; BVerfGE 107, 299, 313; 106, 28, 36.

[123] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; v. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 32, 40.

[124] *Bernsmann* NStZ 2002, 103, 104; *ders./Jansen* StV 1999, 591, 592; *Demko* NStZ 2004, 57, 61; *Günther* NStZ 2005, 485, 491 f.; *Jordan* Kriminalistik 2005, 514, 515.

[125] BGH NJW 2001, 1587; LG Dortmund NStZ 1998, 577; *Bär* MMR 2000, 472, 473; *Dix* Kriminalistik 2004, 81, 83; *Nachbaur* NJW 2007, 335, 337; *Pöppelmann* AfP 2003, 218, 227; *Roggan* KritV 2003, 76, 89 f.; *Schenke* AöR 125 (2000), 1, 20; SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 18.

[126] *Gercke*, a.a.O. (Fn. 19), S. 71; Lisken/Denninger/*Petri*, Hdb. des PolizeiR, 4. Aufl. (2007), H Rn. 12.

[127] BGH NJW 2001, 1587; VG Darmstadt NJW 2001, 2273, 2274; *Dix* Kriminalistik 2004, 81, 83; *Keller*, a.a.O. (Fn. 6), S. 148; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 5; *Nachbaur* NJW 2007, 335, 337.

[128] Vgl. *Gundermann* K&R 1998, 48, 54 f.; *Keller*, a.a.O. (Fn. 6), S. 149 f.; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 5; *Roggan* KritV 2003, 76, 90.

[129] *Gercke*, a.a.O. (Fn. 19), S. 70.

[130] *Schenke* AöR 125 (2000), 1, 20 f.

[131] VG Darmstadt NJW 2001, 2273, 2274; *Bär* MMR 2003, VI, IX; *Denkowski* Kriminalistik 2002, 117, 119; *Dix* Kriminalistik 2004, 81, 83; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 10 Rn. 9; *Nachbaur* NJW 2007, 335, 337; *Roggan* KritV 2003, 76, 90; v. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 45.

[132] BVerfG NJW 2007, 351, 353 f. = HRRS 2006 Nr. 807; *Brenner*, Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern (1994), S. 250; *Jordan* Kriminalistik 2005, 514, 515.

[133] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; *Günther* NStZ 2005, 485, 491.

[134] *Keller*, a.a.O. (Fn. 6), S. 153; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 10 Rn. 2.

[135] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; BVerfG NJW 2006, 976, 978; *Weßlau* ZStW 113 (2001), 681, 690.

[136] Vgl. BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807; *Brenner*, a.a.O. (Fn. 132), S. 251.

[137] Zur Grundrechtsbetroffenheit der Standortermittlung während eines Kommunikationsvorgangs *Keller*, a.a.O. (Fn. 6), S. 151; Lisken/Denninger/*Petri*, a.a.O. (Fn. 126), H Rn. 12.

[138] BVerfG NJW 2007, 351, 353 = HRRS 2006 Nr. 807.

[139] *Bernsmann/Jansen* StV 1999, 591, 592; *Demko* NStZ 2004, 57, 62; *Günther* NStZ 2005, 485, 491; *Jordan* Kriminalistik 2005, 514, 515; *Kudlich* JuS 2001, 1165 ff.; *Weßlau* ZStW 113 (2001), 681, 690.

[140] Unter Verweis auf BVerfG NJW 2007, 351 ff. = HRRS 2006 Nr. 807: *Joecks*, a.a.O. (Fn. 91), § 100i Rn. 2; KK/*Nack*, a.a.O. (Fn. 28), § 100i Rn. 5; *Meyer-Goßner*, a.a.O. (Fn. 74), § 100i Rn. 2; *Pieroth/Schlink*, a.a.O. (Fn. 106), § 19 Rn. 773.

[141] Sachs/*Murswiek*, a.a.O. (Fn. 113), Art. 2 Rn. 73.

[142] BVerfGE 103, 21, 32; 65, 1, 43.

[143] BVerfGE 115, 320, 341; 103, 21, 33; 80, 367, 373; 65, 1, 42; Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 2 I Rn. 78; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 2 Rn. 44.

[144] BVerfG NJW 2007, 351, 354 = HRRS 2006 Nr. 807; BVerfGE 113, 29, 46; 93, 181, 192.

[145] BVerfGE 78, 77, 84; 65, 1, 41 f.; Sachs/*Murswiek*, a.a.O. (Fn. 113), Art. 2 Rn. 73.

[146] BVerfGE 113, 29, 46; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 2 Rn. 45; *Kunig* Jura 1993, 595, 599.

[147] Nach BVerfGE 65, 1, 45 gibt es unter den Bedingungen der automatischen Datenverarbeitung kein belangloses Datum mehr; vgl. *Pieroth/Schlink*, a.a.O. (Fn. 106), § 8 Rn. 377b.

[148] BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807.

[149] BInKommTKG/*Klesczewski*, 1. Aufl. (2006), § 95 Rn. 3.

[150] BVerfGE 76, 171, 192; 60, 234, 241; 54, 129, 138 f.; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 5 Rn. 6.

[151] Dreier/*Schulze-Fielitz*, a.a.O. (Fn. 107), Art. 5 I, II Rn. 75; *Hufen*, a.a.O. (Fn. 106), § 25 Rn. 10; *Pieroth/Schlink*, a.a.O. (Fn. 106), § 13 Rn. 556.

[152] BK/*Degenhart*, GG, Losebl., Stand: 137. Lfg. (Dez. 2008), Art. 5 Rn. 143; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 5 Rn. 7.

[153] *Keller*, a.a.O. (Fn. 6), S. 185.

[154] Vgl. Dreier/*Schulze-Fielitz*, a.a.O. (Fn. 107), Art. 5 I, II Rn. 128; v. Münch/Kunig/*Wendt*, a.a.O. (Fn. 107), Art. 5 Rn. 18.

[155] BK/*Degenhart*, a.a.O. (Fn. 152), Art. 5 Rn. 163; Dreier/*Schulze-Fielitz,* a.a.O. (Fn. 107), Art. 5 I, II Rn. 128; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 5 Rn. 9.

[156] Anders *Keller*, a.a.O. (Fn. 6), S. 186, der danach differenziert, ob es sich um die im Einsatzbereich des IMSI-Catchers befindlichen Personen oder um außenstehende Telekommunikationsteilnehmer handelt.

[157] BVerfGE 97, 332, 340; 80, 137, 152 f.; Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 2 I Rn. 27; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 2 Rn. 2 f.

[158] BVerfG NJW 2007, 351, 356 = HRRS 2006 Nr. 807. – Die Verhinderung von Telekommunikation stellt keinen Eingriff in Art. 10 Abs. 1 GG dar; vgl. Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 10 Rn. 12; v. Mangoldt/Klein/Starck/*Gusy*, a.a.O. (Fn. 107), Art. 10 Rn. 57.

[159] Es handelt sich nicht um einen Fall der Grundrechtskonkurrenz, bei dem die allgemeine Handlungsfreiheit vom spezielleren Recht auf informationelle Selbstbestimmung verdrängt würde. Vorliegend lässt sich die Maßnahme genau genommen in zwei Sachverhalte bzw. zwei Eingriffsrichtungen unterteilen, die jeweils nur ein Grundrecht betreffen. Vgl. Dreier/*Dreier*, a.a.O. (Fn. 107), Vorb. Rn. 155 ff.

[160] Vgl. BVerfG NJW 2007, 351, 354 ff. = HRRS 2006 Nr. 807.

[161] Sachs/*Murswiek*, a.a.O. (Fn. 113), Art. 2 Rn. 101.

[162] BVerfGE 103, 197, 215; 6, 32, 37 ff.; Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 2 I Rn. 54; v. Mangoldt/Klein/Starck/*Starck*, a.a.O. (Fn. 107), Art. 2 Abs. 1 Rn. 25.

[163] Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 2 I Rn. 53, 60; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 2 Rn. 18 f.

[164] Vgl. BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807; *Keller*, a.a.O. (Fn. 6), S. 191.

[165] BVerfGE 113, 348, 366; 64, 72, 79 f.; Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 19 I Rn. 18.

[166] Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 19 Rn. 3.

[167] Dreier/*Dreier*, a.a.O. (Fn. 107), Art. 19 I Rn. 28; v. Mangoldt/Klein/Starck/*Huber*, a.a.O. (Fn. 107), Art. 19 Abs. 1 Rn. 101 ff.

[168] Etwa *Gercke* MMR 2003, 453, 455; *Keller*, a.a.O. (Fn. 6), S. 196; Löwe-Rosenberg/*Schäfer*, a.a.O. (Fn. 7), § 100i Rn. 5; *Roggan* KritV 2003, 76, 89; SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn. 18.

[169] Hingegen wurde die ausdrückliche Zitierung des Art. 10 GG im Rahmen der Neufassung des § 9 Abs. 4 BVerfSchG auch nach dem Urteil des BVerfG aufrechterhalten.

[170] BVerfGE 28, 36, 46; 10, 89, 99; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 19 Rn. 5; Sachs/*Murswiek*, a.a.O. (Fn. 113), Art. 2 Rn. 101; v. Mangoldt/Klein/Starck/*Huber*, a.a.O. (Fn. 107), Art. 19 Abs. 1 Rn. 77.

[171] BVerfGE 10, 89, 99.

[172] BVerfG NJW 2007, 351, 354 = HRRS 2006 Nr. 807; *Joecks*, a.a.O. (Fn. 91), § 100i Rn. 2.

[173] BVerfGE 112, 304, 315; 17, 306, 314; v. Mangoldt/Klein/Starck/*Sommermann*, GG, Band 2, 5. Aufl. (2005), Art. 20 Rn. 289. – Auf Art. 103 Abs. 2 GG kann insoweit nicht zurückgegriffen werden; dieser findet nur auf Normen des materiellen Strafrechts Anwendung.

[174] BVerfGE 110, 33, 53.

[175] BVerfGE 110, 33, 53; 100, 313, 359.

[176] BVerfGE 110, 33, 53; 65, 1, 44.

[177] BVerfGE 113, 348, 375; 110, 33, 54.

[178] BVerfGE 78, 205, 212; 21, 73, 79; *Degenhart*, StaatsR I, 24. Aufl. (2008), Rn. 356.

[179] BVerfGE 21, 73, 78 ff.; 6, 32, 42 f.; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 20 Rn. 58.

[180] BVerfGE 103, 332, 384; 80, 130, 145.

[181] BVerfGE 112, 304, 315 f.; 109, 279, 344; 107, 299, 321; 103, 21, 33 f.; BbgVerfG LKV 1999, 450, 452; SächsVerfGH LKV 1996, 273, 283 f.

[182] Vgl. BVerfGE 103, 21, 34; *Keller*, a.a.O. (Fn. 6), S. 203; KK/*Nack*, a.a.O. (Fn. 28), § 110a Rn. 21.

[183] BVerfGE 112, 304, 316; 103, 21, 34; *Meyer-Goßner*, a.a.O. (Fn. 74), § 98a Rn. 5.

[184] So etwa *Keller*, a.a.O. (Fn. 6), S. 204 ff., 208, der daher einen Verstoß gegen den Bestimmtheitsgrundsatz bejaht. – Vgl. auch *Rieß* GA 2004, 623 ff.; *Welp* GA 2002, 535, 539 f.

[185] SK-StPO/*Wolter*, a.a.O. (Fn. 8), § 100i Rn 11, 27.

[186] *Benfer* MDR 1994, 12; *Meyer-Goßner*, a.a.O. (Fn. 74), § 98a Rn. 5, § 100i Rn. 6.

[187] BVerfGE 107, 299, 322.

[188] A.A. zur alten Rechtslage, *Keller*, a.a.O. (Fn. 6), S. 208, 212. – Das BVerfG NJW 2007, 351 ff. = HRRS 2006 Nr. 807 hat sich mit der Frage der Bestimmtheit des § 100i StPO nicht befasst.

[189] BVerfGE 111, 54, 82; 80, 109, 120; 61, 126, 134.

[190] Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 20 Rn. 83.

[191] *Degenhart*, a.a.O. (Fn. 178), Rn. 399.

[192] BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807.

[193] Vgl. BT-Drs. 14/9088, S. 7.

[194] BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807; BVerfGE 107, 104, 118 f.

[195] BVerfGE 51, 324, 343; 33, 367, 383.

[196] Sachs/*Sachs*, a.a.O. (Fn. 113), Art. 20 Rn. 150; v. Mangoldt/Klein/Starck/*Sommermann*, a.a.O. (Fn. 173), Art. 20 Rn. 314.

[197] *Degenhart*, a.a.O. (Fn. 178), Rn. 401.

[198] Vgl. BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807.

[199] BVerfGE 78, 232, 245; 38, 281, 302; Jarass/Pieroth/*Jarass*, a.a.O. (Fn. 112), Art. 20 Rn. 85.

[200] *Degenhart*, a.a.O. (Fn. 178), Rn. 403.

[201] Dies dürfte wohl an den hohen Kosten und dem höheren Energieverbrauch derartiger GPS-Empfänger liegen; vgl. *Keller*, a.a.O. (Fn. 6), S. 247.

[202] So jedenfalls *Keller*, a.a.O. (Fn. 6), S. 247.

[203] Vgl. *Keller*, a.a.O. (Fn. 6), S. 248.

[204] Problematisch *Keller*, a.a.O. (Fn. 6), S. 249, der den Einsatz der *stillen SMS* als mildere, gleich wirksame Maßnahme nur deshalb ablehnt, weil es derzeit an einer Rechtsgrundlage fehlt. Die grundrechtsbeschränkende Maßnahme wird aber nicht dadurch erforderlich, dass ein gleich geeignetes, milderes Mittel gesetzlich nicht geregelt ist.

[205] Vgl. *Degenhart*, a.a.O. (Fn. 178), Rn. 405.

[206] Vgl. auch BVerfGE 115, 320, 354 ff. = HRRS 2006 Nr. 501 zur Rasterfahndung, mit der auch Eingriffe von großer Streubreite verbunden sind.

[207] BVerfGE 115, 320, 357 ff. = HRRS 2006 Nr. 501, das den Schutz hochrangiger Rechtsgüter fordert.

[208] BVerfGE 33, 367, 383.

[209] BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807; *Hofmann* NStZ 2005, 121.

[210] BVerfGE 46, 214, 222; 33, 367, 383.

[211] Vgl. BVerfG NJW 2007, 351, 355 = HRRS 2006 Nr. 807.

[212] Sondervotum *Haas* BVerfGE 115, 371, 373.

[213] BVerfG NJW 2007, 351, 356 = HRRS 2006 Nr. 807.

[214] BVerfG NJW 2007, 351, 356 = HRRS 2006 Nr. 807. – Vgl. BVerfGE 107, 299, 316 ff.; 100, 313, 388 ff.

[215] Unter Verweis auf die engen Anwendungsvoraussetzungen, den erheblichen Aufwand sowie die von Bundesanwaltschaft und BKA mitgeteilten Zahlen BVerfG NJW 2007, 351, 356 = HRRS 2006 Nr. 807.