Zitierung: BVerfG, 2 BvR 1345/03 vom 22.8.2006, Absatz-Nr. (1 - 85), http://www.bverfg.de/entscheidungen/rk20060822_2bvr134503.html

BUNDESVERFASSUNGSGERICHT

- 2 BvR 1345/03 -

In dem Verfahren
über
die Verfassungsbeschwerde

1. der H ... e.V.,
2. des Herrn Dr. M ...,
3. des Herrn L ...,
4. des Herrn F ...,
5. der verstorbenen Frau Z ...,
6. des Herrn G ...,

- Bevollmächtigte:
Prof. Dr. Rosemarie Will,
Unter den Linden 6, 10099 Berlin -

gegen Art. 1 Nr. 3 des Gesetzes zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl I S. 3018)

hat die 1. Kammer des Zweiten Senats des Bundesverfassungsgerichts durch

den Vizepräsidenten Hassemer,
die Richter Di Fabio
und Landau

gemäß § 93b in Verbindung mit § 93a BVerfGG in der Fassung der Bekanntmachung vom 11. August 1993 (BGBl I S. 1473) am 22. August 2006 einstimmig beschlossen:

Die Verfassungsbeschwerde der Beschwerdeführerin zu 5. hat sich durch ihren Tod erledigt.

Im Übrigen wird die Verfassungsbeschwerde nicht zur Entscheidung angenommen.

Gründe:

A.

1 Die Verfassungsbeschwerde betrifft die Verfassungsmäßigkeit der Ermittlung der Geräte- und Kartennummern sowie des Standorts von Mobiltelefonen durch den so genannten "IMSI-Catcher" (§ 100 i StPO).

I.

2

1. Durch das Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002 (BGBl I S. 3018) wurde § 100 i StPO in die Strafprozessordnung eingeführt. Die Vorschrift lautet in der derzeit geltenden Fassung:

3

> (1) Durch technische Mittel dürfen
>
> 4
>
> zur Vorbereitung einer Maßnahme nach § 100a die Geräte- und Kartennummer sowie
>
> 5
>
> zur vorläufigen Festnahme nach § 127 Abs. 2 oder Ergreifung des Täters auf Grund eines Haftbefehls oder Unterbringungsbefehls der Standort eines aktiv geschalteten Mobilfunkendgerätes ermittelt werden.
>
> 6
>
> (2) Die Maßnahme nach Absatz 1 Nr. 1 ist nur zulässig, wenn die Voraussetzungen des § 100a vorliegen und die Durchführung der Überwachungsmaßnahme ohne die Ermittlung der Geräte- oder Kartennummer nicht möglich oder wesentlich erschwert wäre. Die Maßnahme nach Absatz 1 Nr. 2 ist nur im Falle einer Straftat von erheblicher Bedeutung und nur dann zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder erschwert wäre; § 100f Abs. 3 Satz 2 gilt entsprechend. Die Maßnahme nach Absatz 1 Nr. 2 ist im Falle einer Straftat von erheblicher Bedeutung auch zulässig, wenn die Ermittlung des Aufenthaltsortes des Täters zur Eigensicherung der zur vorläufigen Festnahme oder Ergreifung eingesetzten Beamten des Polizeidienstes erforderlich ist.
>
> 7
>
> (3) Personenbezogene Daten Dritter dürfen anlässlich solcher Maßnahmen nur erhoben werden, wenn dies aus technischen Gründen zur Erreichung des Zwecks nach Absatz 1 unvermeidbar ist. Über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus dürfen sie nicht verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.
>
> 8
>
> (4) § 100b Abs. 1 gilt entsprechend; im Falle der Anordnung zur Vorbereitung einer Maßnahme nach § 100a gilt auch § 100b Abs. 2 Satz 1 entsprechend. Die Anordnung ist auf höchstens sechs Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als sechs weitere Monate ist zulässig, soweit die in den Absätzen 1 und 2 bezeichneten Voraussetzungen fortbestehen. Auf Grund der Anordnung nach Absatz 1 Nr. 2 hat jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, dem Richter, der Staatsanwaltschaft und ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die für die Ermittlung des Standortes des Mobilfunkendgerätes erforderliche Geräte- und Kartennummer mitzuteilen.

9

2. § 100 i Abs. 1 StPO regelt zwei technisch unterschiedliche Ermittlungsmaßnahmen, die im Schrifttum unter dem Stichwort "IMSI-Catcher" diskutiert werden (vgl. Eckhardt, CR 2002, S. 770 <771>; Fox, DuD 2002, S. 212 <213>).

10

a) Maßnahmen nach § 100 i Abs. 1 Nr. 1 StPO ermöglichen die Ermittlung der Gerätenummer (IMEI: International Mobile Equipment Identity) eines Mobilfunkendgeräts (Mobiltelefon) oder der Kartennummer (IMSI: International Mobile Subscriber Identity) einer SIM-Karte (Subscriber Identity Module).

11

aa) Grundlage hierfür ist, dass jedes Mobiltelefon wie auch jede SIM-Karte mit einer weltweit nur einmal

vergebenen Nummer versehen sind (s. hierzu Vassilaki, RDV 2004, S. 11 <14>). Die ersten Ziffern der IMSI bezeichnen den Netzbetreiber; anhand der weiteren Ziffern kann über die beim Netzbetreiber gespeicherten Bestandsdaten (u.a. die Rufnummer, Name und Anschrift des Rufnummerninhabers) der Mobilfunkteilnehmer ermittelt werden (zur Verpflichtung der Netzbetreiber zur Speicherung und Übermittlung dieser Daten an die Strafverfolgungsbehörden s. §§ 113 Abs. 1, 111 TKG). Die Abfrage der Bestandsdaten ist auch mittels der IMEI möglich, was dann von Bedeutung ist, wenn ein Mobiltelefon mit verschiedenen SIM-Karten genutzt wird (vgl. Fox, a.a.O., S. 213). Die Kenntnis der Bestandsdaten ist notwendig für die Anordnung einer Telekommunikationsüberwachung nach § 100 a StPO.

12

Da technische Voraussetzung einer Maßnahme nach § 100 i Abs. 1 Nr. 1 StPO die ungefähre Kenntnis des Standorts eines Mobiltelefons der observierten Person ist (vgl. hierzu Gercke, MMR 2003, S. 453 <454>), kommt der Einsatz eines "IMSI-Catchers" dann in Betracht, wenn bekannt ist, dass an einem bestimmten Ort Mobilfunktelekommunikation betrieben wird, nähere Erkenntnisse über die Identität des Teilnehmers oder das verwendete Mobiltelefon jedoch nicht vorliegen (vgl. Kiper/ Ruhmann, DuD 1998, S. 155 <160>; Roggan, KritV 2003, S. 76 <86 f.>) oder der Benutzer verschiedene SIM-Karten gebraucht (s. hierzu Pöppelmann/Jehmlich, AfP 2003, S. 218 <225>).

13

bb) Die Erfassung der IMSI oder der IMEI macht sich zunutze, dass sich alle Mobiltelefone, die im empfangsbereiten Zustand mitgeführt werden, in kurzen Abständen bei der für sie gerade "zuständigen" Basisstation des Mobilfunknetzes anmelden. Das gesamte Mobilfunknetz ist entsprechend einem Raster in einzelne Zellen aufgeteilt (vgl. Eisenberg/Singelnstein, NStZ 2005, S. 62 Fn 2; Gercke, Bewegungsprofile anhand von Mobilfunkdaten im Strafverfahren, 2002, S. 29 f.). Zum Empfang eingehender Anrufe oder Kurzmitteilungen, wie der des Short Messaging System (SMS), ist daher die genaue Lokalisierung des Standorts des Mobiltelefons durch den Mobilfunknetzbetreiber nötig. Im Rahmen dieser ständigen Positionsangabe werden unter anderem die IMSI und die IMEI an die Basisstation gesendet.

14

Die Erfassung der IMSI und IMEI erfolgt dadurch, dass innerhalb einer solchen Funkzelle eine Basisstation des Mobilfunknetzes durch den "IMSI-Catcher" simuliert wird (vgl. Eckhardt, a.a.O., S. 771; Fox, a.a.O., S. 213). Sämtliche eingeschalteten Mobiltelefone, die sich im Einzugsbereich des "IMSI-Catchers" befinden, senden nunmehr ihre Daten an diesen (von Denkowski, Kriminalistik 2002, S. 117 f.; Gercke, MMR 2003, S. 453 <454>; ders., StraFo 2003, S. 76 <78>; Fox, a.a.O., S. 213; Roggan, a.a.O., S. 86; Vassilaki, a.a.O., S. 14). Dabei ist durch eine verstärkte Sendeleistung diese virtuelle Zelle erheblich kleiner als die reguläre Funkzelle (vgl. hierzu Wolter, in: Systematischer Kommentar zur StPO, 2004, § 100 i Rn. 21). Sofern sich in der simulierten Funkzelle mehrere Mobilfunkteilnehmer befinden, sind zur Bestimmung des gesuchten Mobiltelefons mehrere Messungen erforderlich (vgl. Fox, a.a.O., S. 213). Dabei wird die Messtechnik in den Nahbereich des mutmaßlichen Täters gebracht. Es werden an verschiedenen Orten Messungen durchgeführt und nach einem statistischen Auswerteprinzip in Form von Schnittmengen die jeweiligen IMSI/IMEI ermittelt oder zumindest eingegrenzt (vgl. Virnich, Protokoll der 127. Sitzung des Rechtsausschusses des Deutschen Bundestags vom 24. April 2002, S. 2). Zur eindeutigen Bestimmung des gesuchten Endgeräts können auch ein Abgleich der gemessenen Daten mit den Kundendaten der Mobilfunkbetreiber, ein Stimmenvergleich durch einen Testanruf oder eine Observation der Zielperson nötig sein. Während dieser Zeit bleiben die Daten der erfassten Mobiltelefone – gegebenenfalls auch nur die Daten aus der gebildeten Schnittmenge - gespeichert (s. hierzu von Denkowski, a.a.O., S. 118). Sie sind gemäß § 100 i Abs. 3 StPO nach Beendigung der Maßnahme zu löschen.

15

b) § 100 i Abs. 1 Nr. 2 StPO erlaubt die genaue Standortbestimmung eines Mobiltelefons.

16

aa) Ziel der Maßnahme ist das Auffinden eines Beschuldigten oder Verurteilten zum Zwecke der vorläufigen Festnahme oder Ergreifung aufgrund eines Haft- oder Unterbringungsbefehls. Voraussetzung hierfür ist neben der ungefähren Kenntnis des Standorts, dass die IMSI, die IMEI oder die Telefonnummer des gesuchten Mobiltelefons bekannt sind (s. hierzu von Denkowski, a.a.O., S. 118; Eckhardt, a.a.O., S. 771; Fox, a.a.O., S. 213 f.; Gercke, MMR 2003, S. 453 <454>; Vassilaki, a.a.O., S. 14). Diese dürfen nicht erst aufgrund einer Maßnahme nach § 100 i

Abs. 1 Nr. 1 StPO ermittelt werden, da der Gesetzeswortlaut als Erhebungszweck nur eine Überwachung nach § 100 a StPO zulässt. Allerdings sind nach § 100 i Abs. 4 Satz 4 StPO die Telekommunikationsdienstleister zur Mitteilung der IMSI und IMEI verpflichtet.

17

bb) Die Feststellung des Standorts erfolgt dadurch, dass eine durch den "IMSI-Catcher" aufgebaute virtuelle Funkzelle nach dem Mobiltelefon der Zielperson durchsucht wird. Dabei kann die Suche aufgrund der bereits bekannten Daten von vornherein auf Mobiltelefone beschränkt werden, die dasselbe Netz wie das gesuchte Endgerät verwenden. Auch bei dieser Methode werden nacheinander für einen kurzen Augenblick sämtliche im Einzugsbereich der simulierten Funkzelle befindliche und im selben Netz angemeldete Mobiltelefone erfasst und sofort wieder aussortiert. Ist das gesuchte Mobiltelefon erfasst, sind zur genauen Positionsbestimmung weitere Messungen von verschiedenen Standorten aus erforderlich (vgl. Fox, a.a.O., S. 214; Erläuterung des technischen Vorganges bei Pütz, DuD 1998, S. 462).

18

c) In der Literatur werden auch Modelle des "IMSI-Catchers" erwähnt, die es ermöglichen, sich in Echtzeit in laufende Mobilfunkgespräche einzuschalten und diese mitzuhören (vgl. Fox, a.a.O.).

II.

19

Mit ihrer am 17. Juli 2003 eingegangenen Verfassungsbeschwerde greifen die Beschwerdeführer Art. 1 Nr. 3 des Gesetzes zur Änderung der Strafprozessordnung vom 6. August 2002 an. Sie rügen ausschließlich eine Verletzung von Art. 10 GG.

20

1. Die Beschwerdeführer seien durch § 100 i StPO selbst, gegenwärtig und unmittelbar in Grundrechten betroffen. Sie seien alle Inhaber eines Mobiltelefons. Die Beschwerdeführerin zu 1. sei die älteste und größte Bürgerrechtsorganisation der Bundesrepublik Deutschland. Schwerpunkt ihrer Tätigkeit sei der Schutz der Grundrechte vor staatlichen Übergriffen. Die Beschwerdeführer zu 2. und zu 3. seien Rechtsanwälte, wobei der Beschwerdeführer zu 2. auch als Strafverteidiger tätig sei, der Beschwerdeführer zu 4. sei Pfarrer und kirchlicher Beauftragter für Kriegsdienstverweigerer, die verstorbene Beschwerdeführerin zu 5. war freie Rundfunkjournalistin, und der Beschwerdeführer zu 6. ist freiberuflicher Steuerberater. In ihren beruflichen Funktionen sei es möglich, dass die Strafverfolgungsorgane versuchten, über sie einen Tatverdächtigen zu orten, und zu diesem Zweck die Beschwerdeführer lokalisierten, so dass sie Zielpersonen einer Maßnahme nach § 100 i StPO sein könnten. Auch als unbeteiligte Dritte unterlägen sie wie jeder Mobiltelefonbesitzer dem Risiko, von einer gegen einen anderen gerichteten Maßnahme nach § 100 i StPO erfasst zu werden. Die Beschwerdeführer könnten in den Einzugsbereich eines zur Ortung oder Identifizierung eines anderen eingesetzten "IMSI-Catchers" gelangen, der ihre personenspezifischen Geräte- und Kartenkennungen erfasse und sie identifiziere. Im weiteren Verlauf würden die Daten abgeglichen und vorerst gespeichert, was einen Eingriff in die Fernmeldefreiheit aus Art. 10 GG darstelle. Das Inkrafttreten des § 100 i StPO bringe eine ernsthaft zu besorgende Grundrechtsgefährdung mit sich. Schon das Bewusstsein, anhand eines eingeschalteten Mobiltelefons für die öffentliche Gewalt lokalisierbar zu sein, könne dazu führen, dass die Beschwerdeführer ihre Mobiltelefone ausschalten und damit nicht mehr erreichbar seien. Die Beschwerdeführer seien auch unmittelbar beschwert. Da § 100 i StPO keine Benachrichtigungspflicht vorsehe, bestehe für die Beschwerdeführer keine Möglichkeit, sich gegen die Vollzugsakte als solche zu wenden.

21

2. Die Beschwerdeführer seien in ihrem Grundrecht aus Art. 10 GG verletzt.

22

a) § 100 i StPO verstoße gegen das Zitiergebot (Art. 19 Abs. 1 Satz 2 GG). Die Vorschrift greife in den Schutzbereich des Art. 10 GG ein; ein – hier nicht entbehrlicher - Hinweis darauf fehle im Änderungsgesetz.

23

b) Das Fernmeldegeheimnis aus Art. 10 GG schütze nicht nur den Inhalt, sondern auch alle näheren Umstände des Fernmeldevorgangs und damit auch die Geräte- und Kartennummer sowie die Standortdaten von Mobiltelefonen.

Die Erfassung und Verarbeitung dieser Daten sei ein Eingriff in Art. 10 GG. Die Anwendung des "IMSI-Catchers" sei mit erheblichen Störungen für alle Kommunikationsteilnehmer in der Funkzelle verbunden. Dieser Eingriff sei nicht gerechtfertigt. Denn § 100 i StPO sei nicht Ausdruck des in Art. 10 Abs. 2 Satz 1 GG enthaltenen Gesetzesvorbehalts.

24

c) Die Regelung verletze zudem den Verhältnismäßigkeitsgrundsatz und überschreite die Grundrechtsschranke des Art. 10 GG. Der "IMSI-Catcher" sei zur Erreichung des verfolgten Zwecks ungeeignet. Bereits die Zuordnung einer ermittelten IMSI zur Rufnummer sei nur dann problemlos möglich, wenn es sich um die IMSI eines deutschen Netzbetreibers handele. Bei ausländischen Unternehmen seien die Strafverfolgungsbehörden dagegen auf internationale Rechtshilfeabkommen angewiesen, sofern es denn solche gebe. Der "IMSI-Catcher" könne überdies mit einfachen Mitteln umgangen werden. Einer Peilung könne man sich durch die Benutzung mehrerer Mobiltelefone entziehen. Auch wenn in Deutschland solche Geräte nur gegen Vorlage des Personalausweises verkauft würden, ließen sich diese leicht durch privaten Handel oder durch Diebstahl besorgen. Durch die Verwendung mehrerer Mobiltelefone bestehe dann die Gefahr, dass der "IMSI-Catcher" in unverhältnismäßig großem Umfang eingesetzt würde.

25

Der Erkenntnisgewinn durch die Maßnahme sei relativ gering, da trotz des erheblichen technischen Aufwands lediglich der vermutete Aufenthaltsort verifiziert werde. Zudem werde durch die Maßnahme regelmäßig eine große Zahl völlig Unbeteiligter betroffen. Schließlich trage die Regelung dem in der Strafprozessordnung verankerten Schutz der besonderen Vertrauensverhältnisse keine Rechnung. Dies gelte insbesondere für das Verhältnis zwischen Beschuldigtem und Verteidiger, aber auch zwischen Beschuldigtem und Seelsorger oder Journalisten. Denn § 100 i StPO ermögliche es, einen Beschuldigten über das Mobiltelefon eines mit ihm in Kontakt stehenden Dritten zu orten, auch über seinen Strafverteidiger.

26

d) § 100 i StPO verstoße gegen die aus Art. 10 Abs. 2 Satz 2 GG folgende Benachrichtigungspflicht. Die Vorschrift sehe keine Benachrichtigung der Betroffenen vor. Ohne entsprechende Kenntnis könnten die Betroffenen weder eine mögliche Unrechtmäßigkeit des Eingriffs noch eine etwaige Löschung oder Berichtigung erfasster Daten geltend machen. Dies gelte insbesondere, wenn unbeteiligte Dritte betroffen seien.

27

e) Die Vorschrift verstoße gegen das Bestimmtheitsgebot. Der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürften, müsse bereichspezifisch und präzise bestimmt sein. Der Begriff der "Straftat von erheblicher Bedeutung" in § 100 i Abs. 2 Satz 2 StPO eröffne dagegen einen im Einzelfall nicht mehr hinnehmbar weiten Auslegungsspielraum.

28

3. Unter dem 15. Februar 2006 haben die Beschwerdeführer ihr Vorbringen um die Rüge einer Verletzung des Art. 20 Abs. 1 GG erweitert.

III.

29

1. Zu der Verfassungsbeschwerde haben Stellung genommen das Bundesministerium der Justiz, der Präsident des Bundesgerichtshofs, der Generalbundesanwalt, das Bundeskriminalamt, der Bundesbeauftragte für den Datenschutz, die Niedersächsische Staatskanzlei und der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und der Landesbeauftragte für den Datenschutz Sachsen-Anhalt haben sich der Stellungnahme des Bundesbeauftragten für den Datenschutz angeschlossen. Die Verfahrensbevollmächtigte der Beschwerdeführer hat auf die Stellungnahmen erwidert.

30

Der Präsident des Bundesrats, der Präsident des Deutschen Bundestags, das Justizministerium Mecklenburg-Vorpommern und die Staatskanzlei Sachsen-Anhalt haben mitgeteilt, von einer Stellungnahme abzusehen.

31

2. Der Generalbundesanwalt hat mitgeteilt, dass im Bereich seiner Behörde der "IMSI-Catcher" bislang in vier Ermittlungsverfahren auf der Grundlage des § 100 i Abs. 1 Nr. 1 StPO zum Einsatz gekommen ist. Er habe in drei der Fälle zu wesentlichen Ermittlungserkenntnissen geführt.

32

Die durch die Messungen ermittelten Kennungsdaten von Mobiltelefonen unbeteiligter Dritter seien nach dem Abgleich der Messergebnisse von den technischen Ermittlungsbeamten sofort gelöscht und ausschließlich die Trefferdaten an die sachbearbeitenden Ermittlungsbeamten weitergeleitet worden. Der Messvorgang hinsichtlich des einzelnen Mobiltelefons dauere allenfalls wenige Sekunden, zumal sich jeweils nur ein Mobiltelefon bei dem Messgerät anmelde. Der Messvorgang sei technisch nicht möglich, solange das Mobiltelefon zur Nachrichtenübermittlung (Gespräche, E-Mail, SMS) verwendet werde. Ein zum Zeitpunkt der Messung stattfindender Nachrichtenübermittlungsvorgang könne weder unterbrochen noch aufgezeichnet werden.

33

3. Das Bundesministerium der Justiz hat mitgeteilt, der "IMSI-Catcher" spreche nicht alle Mobiltelefone innerhalb der virtuellen Funkzelle gleichzeitig an; die Mobiltelefone würden vielmehr einzeln und nacheinander erfasst. Zudem gehe das Gerät bei unbekannter IMSI oder IMEI gesondert nach den jeweiligen Netzbetreibern vor. "Festgehalten" werde jedes Mobiltelefon jeweils nur für etwa acht Sekunden während der Anmeldung in der virtuellen Funkzelle. Könne die der Zielperson zuzuordnende IMSI oder IMEI ermittelt werden, so würden die Gerätedaten der anderen Mobiltelefone unverzüglich gelöscht. Gleiches gelte bezüglich aller erfassten Daten, wenn der Einsatz insgesamt erfolglos bleibe.

34

4. Das Bundeskriminalamt hat sich zu den technischen Einzelheiten und zum Umfang des Einsatzes von "IMSI-Catchern" in seinem Geschäftsbereich geäußert.

B.

I.

35

Die Verfassungsbeschwerde ist nur teilweise zulässig.

36

1. Die Verfassungsbeschwerde der Beschwerdeführerin zu 5. hat sich durch ihren Tod erledigt (vgl. BVerfGE 6, 389 <442 f.>; 12, 311 <315>; 109, 279 <304>). Die Fortführung des Verfahrens durch möglicherweise vorhandene Erben wäre nicht zulässig. Eine Rechtsnachfolge im Verfassungsbeschwerdeverfahren kommt grundsätzlich nicht in Betracht, weil diese Verfahrensart regelmäßig der Durchsetzung höchstpersönlicher Rechte dient. Ausnahmen sind im Hinblick auf solche Rügen zugelassen worden, die der Rechtsnachfolger im eigenen Interesse geltend machen kann (vgl. BVerfGE 6, 389 <442 f.>; 17, 86 <90 f.>; 23, 288 <300>; 37, 201 <206>; 69, 188 <201>; 109, 279 <304>). Ein solches zur Fortführung der Verfassungsbeschwerde berechtigendes Interesse wäre für etwaige Erben der Beschwerdeführerin nicht ersichtlich. Die Verfassungsbeschwerde verfolgte allein die Durchsetzung höchstpersönlicher Rechte der Verstorbenen, die maßgeblich an ihre Eigenschaft als freie Rundfunkjournalistin anknüpfen.

37

2. Die "H ... e.V." ist aktivlegitimiert im Sinne des § 90 Abs. 1 BVerfGG. Bei inländischen privatrechtlichen juristischen Personen ist grundsätzlich von einer Grundrechtsfähigkeit und damit Verfassungsbeschwerdefähigkeit auszugehen (vgl. BVerfGE 21, 362 <368>). Art. 10 GG ist weiterhin im Sinne von Art. 19 Abs. 3 GG seinem Wesen nach auch auf juristische Personen anwendbar (vgl. BVerfGE 106, 28 <43>).

38

3. Die Beschwerdeführer sind beschwerdebefugt, soweit sie geltend machen, als unbeteiligte Dritte jederzeit in den Bereich eines "IMSI-Catchers" geraten zu können.

39

a) Den Beschwerdeführern steht die Verfassungsbeschwerde unmittelbar gegen die von ihnen angegriffene gesetzliche Regelung zu.

40

aa) Verfassungsbeschwerde gegen ein Gesetz kann grundsätzlich nur erheben, wer durch die angegriffenen Vorschriften selbst, gegenwärtig und unmittelbar in seinen Grundrechten betroffen ist (vgl. BVerfGE 30, 1 <16>; 90, 128 <135>; 100, 313 <354>; stRspr). Ergibt sich das Betroffensein erst aus der Anwendung des Gesetzes, so können Verfassungsbeschwerden nicht gegen das Gesetz, sondern nur gegen den Vollzugsakt gerichtet werden. An der Möglichkeit, den Vollzugsakt anzugreifen, fehlt es allerdings dann, wenn der Betroffene keine Kenntnis davon erlangen kann. In diesem Fall muss ihm die Verfassungsbeschwerde unmittelbar gegen das Gesetz ebenso zustehen wie in jenen Fällen, in denen die grundrechtliche Beschwer ohne vermittelnden Vollzugsakt durch das Gesetz selbst eintritt (vgl. BVerfGE 30, 1 <16 f.>; 100, 313 <354>; 109, 279 <306 f.>).

41

bb) § 100 i StPO sieht keine Benachrichtigungspflicht vor. Mangels Kenntnis eines etwaigen Vollzugsaktes haben die Beschwerdeführer keine Möglichkeit, sich gegen einen solchen zu wenden.

42

b) Die Beschwerdeführer haben auch ihr persönliches und unmittelbares Betroffensein hinreichend dargelegt, soweit sie geltend machen, als unbeteiligte Dritte jederzeit in den Bereich eines "IMSI-Catchers" geraten zu können.

43

aa) Die Anforderungen an die Begründung der Verfassungsbeschwerde nach § 23 Abs. 1 Satz 2, § 92 BVerfGG sind erfüllt, wenn der Beschwerdeführer darlegt, dass er mit einiger Wahrscheinlichkeit durch Maßnahmen, die auf den angegriffenen Rechtsnormen beruhen, in seinen Grundrechten berührt wird (vgl. BVerfGE 67, 157 <169 f.>; 100, 313 <354>; 109, 279 <307 f.>). Der geforderte Grad der Wahrscheinlichkeit ist davon abhängig, welche Möglichkeit der Beschwerdeführer hat, sein Betroffensein darzulegen. Insofern ist es bedeutsam, ob die Maßnahme auf einen tatbestandlich eng umgrenzten Personenkreis zielt oder ob sie eine große Streubreite hat und Dritte auch zufällig erfassen kann (vgl. BVerfGE 109, 279 <308>).

44

bb) Das Vorbringen der Beschwerdeführer genügt diesen Darlegungsvoraussetzungen jedenfalls, soweit sie geltend machen, als unbeteiligte Dritte jederzeit in den Bereich eines "IMSI-Catchers" geraten zu können. Durch Ermittlungsmaßnahmen nach § 100 i StPO werden die in einer simulierten Funkzelle befindlichen empfangsbereit gehaltenen Mobiltelefone erfasst. Grundsätzlich kann sich jedermann im Bereich einer solchen Zelle befinden und allein aufgrund des Mitführens eines Mobiltelefons auch als Unbeteiligter Grundrechtsbetroffener sein. Sämtliche Beschwerdeführer sind im Besitz eines Mobiltelefons. Eine weitere Substantiierung der Betroffenheit ist vor diesem Hintergrund weder möglich noch erforderlich (vgl. BVerfGE 109, 279 <308>).

45

cc) Vor diesem Hintergrund kann dahinstehen, ob die Beschwerdeführer hinreichend substantiiert dargelegt haben, die Strafverfolgungsorgane könnten mit einiger Wahrscheinlichkeit versuchen, sie im Rahmen bestehender Vertrauensverhältnisse - insbesondere in ihrer Eigenschaft als Strafverteidiger von Beschuldigten, die einer Straftat im Sinne des § 100 i StPO verdächtig sind - als Verbindungsperson eines "Täters" zu orten.

46

dd) Dass die Beschwerdeführer im Übrigen selbst Zielpersonen einer Maßnahme nach § 100 i Abs. 1 Nr. 2 StPO sein könnten, behaupten sie nicht.

47

4. Soweit die Beschwerdeführer ihr Vorbringen um die Verletzung des Art. 20 Abs. 1 GG ergänzt haben, ist diese Rüge unzulässig, da es sich nicht um ein rügefähiges Grundrecht oder grundrechtsgleiches Recht handelt (Art. 93 Abs. 1 Nr. 4 a GG).

II.

48

Soweit zulässig, ist die Verfassungsbeschwerde unbegründet.

49

1. Die Beschwerdeführer sind durch die Bestimmung des § 100 i Abs. 1 StPO nicht in ihrem Grundrecht aus Art. 10 Abs. 1 GG verletzt. Die Erhebung der Daten, durch die aufgrund dieser Vorschrift zugegriffen werden darf, fällt nicht in den Schutzbereich des Art. 10 Abs. 1 GG.

50

a) Brief-, Post- und Fernmeldegeheimnis gewährleisten die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Nachrichten, Gedanken und Meinungen als Informationen (vgl. BVerfGE 67, 157 <171>; 106, 28 <35 f.>; 110, 33 <53>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, S. 976 <977>; Dürig, in: Maunz/Dürig, Grundgesetz, Loseblatt <Stand: Dezember 1973>, Art. 10 Rn. 1).

51

aa) Art. 10 GG schützt die private Fernkommunikation. Brief-, Post- und Fernmeldegeheimnis gewährleisten die Vertraulichkeit der individuellen Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere angewiesen ist und deshalb in besonderer Weise einen Zugriff Dritter - einschließlich staatlicher Stellen - ermöglicht. Brief-, Post- und Fernmeldegeheimnis sind wesentlicher Bestandteil des Schutzes der Privatsphäre; sie schützen vor ungewollter Informationserhebung und gewährleisten eine Privatheit auf Distanz (vgl. Gusy, in: von Mangoldt/Klein/ Starck, Grundgesetz, 5. Aufl. 2005, Art. 10 Rn. 19). Das Fernmeldegeheimnis schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs (vgl. BVerfGE 67, 157 <172>; 106, 28 <35 f.>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, S. 976 <978>). Die Beteiligten sollen weitestgehend so gestellt werden wie sie bei einer Kommunikation unter Anwesenden stünden. Das Grundrecht ist entwicklungsoffen und umfasst nicht nur die bei Entstehung des Gesetzes bekannten Arten der Nachrichtenübertragung, sondern auch neuartige Übertragungstechniken (vgl. BVerfGE 46, 120 <144>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, a.a.O.). Die Reichweite des Grundrechts beschränkt sich daher nicht auf die früher von der Deutschen Bundespost angebotenen Fernmeldedienste, sondern erstreckt sich auf jede Übermittlung von Informationen mit Hilfe der verfügbaren Telekommunikationstechniken. Auf die konkrete Übermittlungsart (Kabel oder Funk, analoge oder digitale Vermittlung) und Ausdrucksform (Sprache, Bilder, Töne, Zeichen oder sonstige Daten) kommt es nicht an (vgl. BVerfGE 106, 28 <36>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, a.a.O.). Der Schutzbereich des Fernmeldegeheimnisses umfasst sowohl den Inhalt der Telekommunikation als auch die näheren Umstände des Fernmeldevorgangs, allerdings nur, soweit diese überhaupt auf Kommunikationsinhalte beziehbar sind (vgl. Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, a.a.O.).

52

bb) Das Fernmeldegeheimnis schützt in erster Linie die Vertraulichkeit der ausgetauschten Informationen und damit den Kommunikationsinhalt gegen unbefugte Kenntniserlangung durch Dritte (vgl. BVerfGE 100, 313 <358>; 107, 299 <312>). Als Folge der Digitalisierung hinterlässt vor allem jede Nutzung der Telekommunikation personenbezogene Spuren, die gespeichert und ausgewertet werden können. Auch der Zugriff auf diese Daten fällt in den Schutzbereich des Art. 10 GG; das Grundrecht schützt auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs (vgl. BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312>; 110, 33 <53>; 113, 348 <364 f.>). Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist (BVerfGE 100, 313 <358>; 107, 299 <312 f.>). Auch insoweit kann der Staat grundsätzlich keine Kenntnis beanspruchen. Die Nutzung des Kommunikationsmediums soll in allem vertraulich sein (BVerfGE 100, 313 <358>; Beschluss der 3. Kammer des Zweiten Senats des Bundesverfassungsgerichts vom 17. Juni 2006 – 2 BvR 1085/05, 2 BvR 1189/05 -). Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen (vgl. dazu BVerfGE 107, 299 <314, 320>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, a.a.O.).

53

Post und Telekommunikation bieten die Voraussetzungen für die private Kommunikation zwischen Personen, die nicht am selben Ort sind, und eröffnen so eine neue Dimension der Privatsphäre (vgl. Gusy, in: von Mangoldt/Klein/Starck, Grundgesetz, 5. Aufl. 2005, Art. 10 Rn. 18 f.). Damit verbunden ist ein Verlust an Privatheit; denn die Kommunizierenden müssen sich auf die technischen Besonderheiten eines Kommunikationsmediums einlassen und sich dem eingeschalteten Kommunikationsmittler anvertrauen. Inhalt und Umstände der Nachrichtenübermittlung sind dadurch dem erleichterten Zugriff Dritter ausgesetzt. Die Beteiligten, die ihre Kommunikation mit Hilfe von technischen Hilfsmitteln über Distanz unter Nutzung fremder Kommunikationsverbindungswege ausüben, haben nicht die Möglichkeit, die Vertraulichkeit der Kommunikation sicherzustellen.

54

Art. 10 Abs. 1 GG soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und will den Gefahren begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben (vgl. BVerfGE 85, 386 <396>; 106, 28 <36>; 107, 299 <313>). Das Fernmeldegeheimnis knüpft an das Kommunikationsmedium an (vgl. BVerfGE 100, 313 <363>; Gusy, in: von Mangoldt/Klein/Starck, Grundgesetz, 5. Aufl. 2005, Art. 10 Rn. 32 und 40; Hermes, in: Dreier, Grundgesetz, 2. Aufl. 2004, Art. 10 Rn. 25).

55

b) Die Datenerhebung nach § 100 i StPO greift nicht in den Schutzbereich der Telekommunikationsfreiheit ein. Sie steht nicht im Zusammenhang mit einem Kommunikationsvorgang und betrifft auch keinen Kommunikationsinhalt im Sinne des Art. 10 Abs. 1 GG.

56

aa) Im Falle einer Maßnahme nach § 100 i Abs. 1 Nr. 2 StPO sind den Strafverfolgungsbehörden die Betriebsdaten bereits bekannt. Es wird lediglich der genaue Standort des Mobiltelefons bestimmt.

57

bb) Die Feststellung einer Geräte- oder Kartennummer im Sinne des § 100 i Abs. 1 Nr. 1 StPO eines im Bereich einer simulierten Funkzelle befindlichen Mobiltelefons durch den Einsatz eines "IMSI-Catchers" ist unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen (vgl. Günther, NStZ 2005, S. 485 Fn 1, 491; Jordan, Kriminalistik 2005, S. 514 <515 f.>; Demko, NStZ 2004, S. 57 <61>; Eisenberg/Singelnstein, NStZ 2005, S. 62 <66>; Bernsmann, NStZ 2002, S. 103; Günther, Kriminalistik 2004, S. 11 <14>; Weßlau, ZStW Bd. 113 <2001>, S. 681 <690>; Kudlich, JuS 2001, S. 1165 <1168>). Beim Einsatz des "IMSI-Catchers" "kommunizieren" ausschließlich technische Geräte miteinander. Es fehlt an einem menschlich veranlassten Informationsaustausch, der sich auf Kommunikationsinhalte bezieht. Das Aussenden der Daten erfolgt unabhängig von einem konkreten Kommunikationsvorgang oder dem Aufbau einer Kommunikationsverbindung, die einen personalen Bezug hat; der Datenaustausch ist ausschließlich zur Sicherung der Betriebsbereitschaft nötig, trägt aber keine individuellen und kommunikativen Züge. Die erfassten Daten fallen nicht anlässlich eines Kommunikationsvorgangs an, sondern im Bereitschaftszustand eines Mobiltelefons, der erst technische Voraussetzung eines Kommunikationsvorgangs ist. Die bloße technische Eignung eines Geräts, als Kommunikationsmittel zu dienen, sowie die von dem Gerät ausgehenden technischen Signale zur Gewährleistung der Kommunikationsbereitschaft stellen noch keine Kommunikation dar. Sie ermöglichen – anders als Kommunikationsumstände - keinen Rückschluss auf Kommunikationsbeziehungen und –inhalte, sondern lediglich über die Position eines Endgeräts auf den Standort einer Person. Erst die tatsächliche Nutzung zum Austausch von Informationen und Meinungen qualifiziert die mittels Telekommunikationseinrichtungen übertragenen Daten als Kommunikationsinhalte und –umstände, die den Schutz des Art. 10 Abs. 1 GG genießen (vgl. Günther, Kriminalistik 2004, S. 11 <14>) und auf die nur unter den engeren Voraussetzungen der §§ 100 a, 100 b, 100 g und 100 h StPO zugegriffen werden darf. Die technischen Signale, die die Kommunikationsbereitschaft gewährleisten, stellen dagegen lediglich Spuren derselben dar (vgl. Weßlau, a.a.O.).

58

Für diese Ansicht spricht zudem, dass nach § 88 Abs. 1 TKG – ungeachtet der jeweils unterschiedlichen Regelungsbereiche von Telekommunikationsgesetz, Strafprozessordnung und Grundgesetz - der Inhalt der Telekommunikation und ihre näheren Umstände dem Fernmeldegeheimnis unterliegen, insbesondere, ob "jemand" an einem Telekommunikationsvorgang beteiligt ist, wobei auch erfolglose Verbindungsversuche erfasst werden. Auch diese Formulierung bringt den personalen Bezug des Fernmeldegeheimnisses und des Schutzbereichs der

Telekommunikationsfreiheit zum Ausdruck.

59

cc) Die Positionsmeldungen eines Mobiltelefons unter den Schutz des Art. 10 Abs. 1 GG fassende Gegenansicht (vgl. Bundesgerichtshof, Ermittlungsrichter, Beschluss vom 21. Februar 2001 – 2 BGs 42/01 -, NJW 2001, S. 1587 mit Anm. Bernsmann, NStZ 2002, S. 103 f.; Bundesgerichtshof, Urteil vom 14. März 2003 - 2 StR 341/02 -, NJW 2003, S. 2034 <2035>; Landgericht Dortmund, Beschluss vom 28. Oktober 1997 – 79 Js 449-97 -, NStZ 1998, S. 577; Landgericht Aachen, Beschluss vom 24. November 1998 – 64 Qs 78/98 -, StV 1999, S. 590 <591>; Verwaltungsgericht Darmstadt, Gerichtsbescheid vom 16. November 2000 – 3 E 915/99 -, NJW 2001, S. 2273 <2274>; Gercke, MMR 2003, S. 453 <455>; ders., StraFo 2003, S. 76 <78>; Schenke, AöR 125 <2000>, S. 1 <20>; hierzu auch Roggan, KritV 2003, S. 76 <89>; Gundermann, K&R 1998, S. 48 <55>; Wolter, in: Systematischer Kommentar zur StPO, 2004, § 100 i Rn. 18; von Denkowski, Kriminalistik 2002, S. 117 <119>; Löwnau-Iqbal, DuD 2001, S. 578; Dix, Kriminalistik 2004, S. 81 <83>; vgl. auch Schäfer, in: Löwe-Rosenberg, StPO, 25. Aufl., § 100 i Rn. 5) lässt außer Acht, dass eine technische Kommunikation zwischen Geräten nicht das spezifische Gefahrenpotential aufweist, vor dem Art. 10 Abs. 1 GG Schutz gewährleistet. Art. 10 Abs. 1 GG folgt nicht dem rein technischen Telekommunikationsbegriff des Telekommunikationsgesetzes (vgl. § 3 Nr. 22 TKG), sondern knüpft personal an den Grundrechtsträger und dessen Schutzbedürftigkeit aufgrund der Einschaltung Dritter in den Kommunikationsvorgang an. Die Erfassung der IMSI und der IMEI mag somit zwar die Bereitschaft zur Nutzung eines Mobiltelefons beeinträchtigen, realisiert aber nicht die spezifischen Gefahren für die Privatheit der Kommunikation, die in der Nutzung des Telekommunikationsmediums begründet liegen.

60

Dass der Besitzer eines Mobiltelefons gewärtigen muss, schon seine Bereitschaft zu einem Kommunikationsvorgang könnte dazu benutzt werden, sich in Kenntnis der Geräte- und Kartennummer seines Mobiltelefons, seiner Identität sowie seines ungefähren Aufenthaltsorts zu setzen, betrifft zwar gegebenenfalls sein Recht auf informationelle Selbstbestimmung und seine allgemeine Handlungsfreiheit, schränkt aber nicht die Bedingungen freier Telekommunikation ein.

61

Zwar verfügt der potentielle Kommunikationsteilnehmer nicht über die gleiche Sicherheit, die bestünde, wenn er sich bei der beabsichtigten Kommunikation keines technischen Mediums bediente. Die Privatheit der Kommunikation in Bezug auf ihre konkreten Umstände ist aber nicht bereits durch die Ausforschung der Kommunikationsbereitschaft gefährdet. Neben dem eigentlichen Kommunikationsvorgang verdient die vorgelagerte Kommunikationsanbahnung nicht den gleichen Schutz. Ein "Für-möglich-halten" von Kommunikation stellt noch keine solche dar (vgl. hierzu Jordan, a.a.O., S. 516).

62

dd) Beim Einsatz des "IMSI-Catchers" werden die IMSI- und IMEI-Daten zudem nicht innerhalb des Herrschaftsbereichs eines Telekommunikationsunternehmens, sondern ohne dessen Mitwirkung durch die Strafverfolgungsbehörden selbst und unmittelbar erhoben. Mit dem Einsatz des "IMSI-Catchers" schaffen diese eine netzexterne, gleichsam virtuelle Funkzelle, die die Erhebung der Daten ermöglicht. Nach dem Grundverständnis des Art. 10 Abs. 1 GG, der insbesondere die erhöhte Verletzlichkeit und Überwachungsanfälligkeit des Übertragungsvorgangs durch die Einschaltung Dritter schützt, unterfallen die hierbei erhobenen Daten nicht dem Telekommunikationsgeheimnis.

63

c) Ist der Schutzbereich des Art. 10 GG nicht eröffnet, so liegt auch kein Verstoß gegen das Zitiergebot des Art. 19 Abs. 1 Satz 2 GG vor. Zwar hat der Erste Senat des Bundesverfassungsgerichts in seiner Entscheidung vom 27. Juli 2005 (1 BvR 668/04, BVerfGE 113, 348 <372>) ausgeführt, der Bundesgesetzgeber habe die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung in den §§ 100 a, 100 b, 100 g, 100 h und 100 i StPO nach Umfang, Zuständigkeit und Zweck sowie hinsichtlich der für die jeweilige Maßnahme erforderlichen Voraussetzungen umfassend geregelt. Aus dem Zusammenhang der Ausführungen ergibt sich jedoch, dass der Senat die besonderen Gegebenheiten der § 100 i StPO zugrunde liegenden Maßnahmen nicht näher behandelt hat, zumal die Maßnahme nach § 100 i StPO unter anderem der Vorbereitung einer Telekommunikationsüberwachung dient und daher einfachgesetzlich den entsprechenden Regelungen zugerechnet werden kann. Das bedeutet aber nicht, dass die Maßnahme selbst dem Schutzbereich des Art. 10 Abs. 1 GG unterfällt.

64

2. Im Übrigen haben die Beschwerdeführer weder ausdrücklich vorgetragen noch ist sonst ersichtlich, dass § 100 i Abs. 1 StPO, soweit Daten unbeteiligter Dritter erhoben werden, ihr Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG verletzt. Der Eingriff in dieses Recht durch die Erhebung und die kurzzeitige Speicherung der IMSI- und IMEI-Kennung der Mobiltelefone der Beschwerdeführer als unbeteiligte Dritte bei Einsatz eines "IMSI-Catchers" beruht mit § 100 i StPO auf einer wirksam zu Stande gekommenen gesetzlichen Grundlage und ist nicht unverhältnismäßig.

65

a) Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist von dem Grundrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG verbürgt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen (vgl. BVerfGE 65, 1 <43>). Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden. Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist (vgl. BVerfG, a.a.O.).

66

aa) Fernmeldegeheimnis und Recht auf informationelle Selbstbestimmung stehen, soweit es um den Schutz der technischen Kommunikationsdaten geht, in einem Ergänzungsverhältnis. In seinem Anwendungsbereich enthält Art. 10 GG bezogen auf den Fernmeldeverkehr eine spezielle Garantie, die die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt (vgl. BVerfGE 67, 157 <171>; 100, 313 <358>; 107, 299 <312>; 110, 33 <53>; 113, 348 <364>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, S. 976 <979>). Soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind dabei die Maßgaben, die das Bundesverfassungsgericht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG entwickelt hat (vgl. BVerfGE 65, 1 <44 ff.>), grundsätzlich auch auf die speziellere Garantie in Art. 10 Abs. 1 GG zu übertragen (vgl. BVerfGE 100, 313 <359>; 110, 33 <53>; Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, S. 976 <979 f.>).

67

bb) Greift Art. 10 GG nicht ein, werden die technischen Kommunikationsdaten durch das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützt. Damit wird der besonderen Schutzwürdigkeit der Daten im Zusammenhang mit Telekommunikation Rechnung getragen.

68

cc) Bei IMSI und IMEI eines Mobiltelefons handelt es sich um personenbeziehbare Daten, die - gegebenenfalls mittels eines Auskunftsersuchens an den Telekommunikationsanbieter - einen Schluss darauf zulassen, welche Person sich im Bereich der virtuellen Funkzelle aufhält. Durch die Maßnahme nach § 100 i Abs. 1 Nr. 2 StPO kann der genaue Standort einer Person bestimmt werden.

69

b) Beschränkungen des Art. 2 Abs. 1 GG bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht (vgl. Beschluss des Zweiten Senats des Bundesverfassungsgerichts vom 12. April 2005 - 2 BvR 1027/02 -, NJW 2005, S. 1917 <1919>). Das Zustandekommen des § 100 i Abs. 1 StPO entspricht den verfassungsrechtlichen Vorgaben (aa); auch unter Verhältnismäßigkeitsgesichtspunkten hält die Norm hinsichtlich des Betroffenseins unbeteiligter Dritter verfassungsrechtlicher Prüfung stand (bb).

70

aa) Die Vorschrift ist in einem Gesetzgebungsverfahren zu Stande gekommen, das nicht an einem durchgreifenden Fehler leidet. Weil die Notwendigkeit und die nähere Ausgestaltung einer gesetzlichen Regelung zum Einsatz des "IMSI-Catchers" bereits Gegenstand eines Änderungsvorschlags des Bundesrats zum Gesetzentwurf der Bundesregierung für ein Begleitgesetz zum Telekommunikationsgesetz vom 23. Mai 1997 war, hatten Parlament und Öffentlichkeit bis zum Gesetzgebungsverfahren im Jahre 2002 ausreichend Gelegenheit, sich mit einer solchen Regelung auseinanderzusetzen. Im Hinblick auf das Zustandekommen des Gesetzes zur Änderung der Strafprozessordnung vom 6. August 2002 entspricht es parlamentarischer Übung, Änderungen und Ergänzungen nach der ersten Lesung eines Gesetzentwurfs in den Ausschussberatungen anzubringen. Auch wenn eine Behandlung des vollständigen Gesetzentwurfs bereits in der ersten Lesung dem Gebot der Öffentlichkeit und Transparenz des Gesetzgebungsvorgangs in höherem Maße gerecht geworden wäre, kommt es für das Wirksamwerden des Gesetzes zunächst nur auf den nach der parlamentarischen Beratung nach Art. 77 Abs. 1 Satz 1 in Verbindung mit Art. 42 Abs. 2 Satz 1 GG gefassten Gesetzesbeschluss des Bundestags an. In der Gestaltung des dahin führenden Verfahrens ist der Bundestag im Rahmen seiner Geschäftsordnungsautonomie frei (vgl. BVerfGE 10, 4 <19>; 80, 188 <220>; 84, 304 <322>).

71

bb) Der Grundsatz der Verhältnismäßigkeit verlangt, dass die jeweilige Maßnahme einen verfassungsrechtlich legitimen Zweck verfolgt und zu dessen Erreichung geeignet, erforderlich und im engeren Sinne verhältnismäßig ist; der Eingriff darf den Betroffenen nicht übermäßig belasten, muss diesem also zumutbar sein (vgl. BVerfGE 63, 131 <144>).

72

(1) Wirksame Strafverfolgung ist ein legitimer Zweck zur Einschränkung des Rechts auf informationelle Selbstbestimmung. Die Sicherung des Rechtsfriedens durch Strafrecht ist seit jeher eine wichtige Aufgabe staatlicher Gewalt. Die Aufklärung von Straftaten, die Ermittlung des Täters, die Feststellung seiner Schuld und seine Bestrafung wie auch der Freispruch des Unschuldigen sind die wesentlichen Aufgaben der Strafrechtspflege, die zum Schutz der Bürger den staatlichen Strafanspruch in einem justizförmigen und auf die Ermittlung der Wahrheit ausgerichteten Verfahren in gleichförmiger Weise durchsetzen soll. Die Schaffung von Strafnormen und deren Anwendung in einem rechtsstaatlichen Verfahren sind Verfassungsaufgaben (vgl. BVerfGE 107, 104 <118 f.> m.w.N.). Der Verhinderung und Aufklärung von Straftaten kommt daher nach dem Grundgesetz eine hohe Bedeutung zu (vgl. BVerfGE 100, 313 <388>).

73

(2) Die Möglichkeit, zur Vorbereitung einer Maßnahme nach § 100 a StPO die Geräte- und Kartennummer oder zur vorläufigen Festnahme nach § 127 Abs. 2 StPO oder Ergreifung des Täters aufgrund eines Haftbefehls oder Unterbringungsbefehls den Standort eines aktiv geschalteten Mobilfunkendgeräts zu ermitteln, ist zur Erreichung dieses Ziels nicht nur geeignet und erforderlich, sondern auch angemessen.

74

Der Einsatz des "IMSI-Catchers" ist zum Zwecke der Aufklärung und Verfolgung von Straftaten geeignet. Er ermöglicht die Feststellung bislang unbekannter Geräte- und SIM-Kartennummern und erlaubt damit eine Zuordnung der Rufnummer zu dem von einem Tatverdächtigen benutzten Mobiltelefon als notwendige Voraussetzung für die Anordnung und Durchführung einer Telekommunikationsüberwachung nach § 100 a StPO. Berichte aus der kriminalistischen Praxis belegen die Geeignetheit und Erforderlichkeit des kriminaltechnischen Hilfsmittels "IMSI-Catcher" (vgl. von Denkowski, Kriminalistik 2002, S. 117 <118 f.>; Albrecht/ Dorsch/Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen, Freiburg 2003, S. 199 f., 216). Dies wird auch durch die im vorliegenden Verfassungsbeschwerdeverfahren abgegebenen Stellungnahmen des Generalbundesanwalts und des Bundeskriminalamts bestätigt, die die Bedeutung dieser Ermittlungsmaßnahme hervorheben. Technische und faktische Schwierigkeiten, die etwa durch den Wechsel von Telefonen und SIM-Karten oder die Verwendung ausländischer SIM-Karten durch die Beschuldigten sowie durch den sachlichen und personellen Aufwand der Maßnahme verursacht sein können, stellen die grundsätzliche Geeignetheit und die Erforderlichkeit des Mittels zur Erreichung des angestrebten Zwecks nicht in Frage.

75

Die Beschwerdeführer werden durch den Einsatz des "IMSI-Catchers" auch nicht übermäßig in ihrem Recht auf

informationelle Selbstbestimmung betroffen. Dabei ist einerseits zu berücksichtigen, dass auch die technischen Kommunikationsdaten einen schutzwürdigen Aussagegehalt haben, weil sie – wenn auch nur nach vorausgegangener Identifizierung der Person über eine Zuordnung der IMSI- oder IMEI-Nummer - einen Schluss darauf zulassen, welche Person sich im Bereich der virtuellen Funkzelle aufhält und ein betriebsbereites Mobiltelefon mit sich führt. Andererseits ist in Rechnung zu stellen, dass die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche die Strafverfolgung erschwert hat. Moderne Kommunikationstechniken werden bei der Begehung unterschiedlichster Straftaten zunehmend eingesetzt und tragen dort zur Effektivierung krimineller Handlungen bei (vgl. Hofmann, NStZ 2005, S. 121). Das Schritthalten der Strafverfolgungsbehörden mit dem technischen Fortschritt kann daher nicht lediglich als sinnvolle Abrundung des Arsenals kriminalistischer Ermittlungsmethoden begriffen werden, die weiterhin wirkungsvolle herkömmliche Ermittlungsmaßnahmen ergänzt, sondern ist vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr einschließlich der anschließenden digitalen Verarbeitung und Speicherung zu sehen (vgl. Urteil des Zweiten Senats des Bundesverfassungsgerichts vom 2. März 2006 - 2 BvR 2099/04 -, NJW 2006, S. 976 <980 f.>).

76

Bei der Durchführung von Maßnahmen nach § 100 i StPO haben die Ermittlungsbehörden darauf Bedacht zu nehmen, dass die Grundrechtspositionen der unbeteiligten Dritten nicht über das unbedingt notwendige Maß hinaus berührt werden. Anhaltspunkte für eine Missachtung dieses Gebots haben sich aus den Stellungnahmen der Äußerungsberechtigten im Verfassungsbeschwerdeverfahren nicht ergeben. Die technischen Kommunikationsdaten werden automatisch und anonym abgeglichen und unverzüglich gelöscht. Unbeteiligte Dritte werden nach Auskunft des Bundeskriminalamts nicht identifiziert. Die Speicherung ihrer Daten erfolgt maximal für die Dauer des Messeinsatzes. Danach werden die Daten von der Festplatte des Messsystems ohne weitere Bearbeitung und Prüfung unverzüglich und unwiderruflich gelöscht.

77

(3) Angesichts der geringen Eingriffsintensität ist es nicht unverhältnismäßig, auf die Benachrichtigung mitbetroffener Dritter zu verzichten (vgl. § 98 b Abs. 4 Satz 1, § 163 d Abs. 5 StPO, hierzu Schoreit, in: Karlsruher Kommentar zur StPO, 5. Aufl. 2003, § 163 d Rn. 44 StPO). Die IMSI- und die IMEI-Nummer können erst mit Hilfe der Netzbetreiber einer Rufnummer bzw. einer Person zugeordnet werden. Eine Benachrichtigung würde daher erfordern, diesen Personenbezug zu ermitteln, was den Grundrechtseingriff noch vertiefen würde (vgl. BVerfGE 109, 279 <365>). In einer solchen Deanonymisierung läge ein schwerer wiegender Eingriff für die auf diese Weise mit Ort, Zeit und Empfangsbereitschaft ihres Mobiltelefons identifizierten Dritten gegenüber der kurzzeitigen Aufnahme der Gerätekennung, die keiner Person zugeordnet ist und nach anonymem Abgleich mit anderen Kennungen sofort unter strikter Beachtung des § 100 i Abs. 3 StPO zu löschen ist. Außerdem würden die Nachforschungen zur Identität des mitbetroffenen Dritten einen erheblichen Aufwand verursachen, zumal der Benutzer des Telefons im Zeitpunkt des Einsatzes des "IMSI-Catchers" nicht mit derjenigen Person identisch sein muss, auf deren Namen das Mobiltelefon oder die SIM-Karte registriert sind.

78

cc) Sollten bei den Ermittlungsbehörden "IMSI-Catcher" vorhanden sein, die technisch ein Mithören von Telefongesprächen in Echtzeit ermöglichen, so wäre die Nutzung dieser Funktion nicht durch § 100 i StPO gedeckt.

79

3. Auch ein Eingriff in die durch Art. 2 Abs. 1 GG gewährleistete allgemeine Handlungsfreiheit der Beschwerdeführer ist weder ausdrücklich vorgetragen noch sonst ersichtlich.

80

a) Soweit durch den Einsatz des "IMSI-Catchers" für einige Sekunden die Herstellung einer Telekommunikationsverbindung für ein einzelnes Mobiltelefon nicht möglich ist, handelt es sich um eine Verhinderung von Telekommunikation, die nicht unter Art. 10 Abs. 1 GG fällt (vgl. Jarass, in: Jarass/Pieroth, Grundgesetz, 8. Aufl. 2006, Art. 10 Rn. 12). Das Unterbinden von Telekommunikation ist daher am Grundrecht der allgemeinen Handlungsfreiheit zu messen, das Betätigungen jedweder Art schützt (vgl. Dreier, in: Dreier, Grundgesetz, 2. Aufl. 2004, Art. 2 Rn. 27).

81

b) Die Beeinträchtigung der Grundrechtsposition unbeteiligter Dritter ist jedenfalls gerechtfertigt.

82

aa) Laufende Gespräche oder anderweitige Kommunikationsverbindungen werden wegen der Funktionsweise des "IMSI-Catchers" nicht gestört, so dass insoweit schon kein Eingriff vorliegt. Angesichts der engen Anwendungsvoraussetzungen und des infolge des erheblichen Aufwands – nach den vom Generalbundesanwalt und dem Bundeskriminalamt mitgeteilten Zahlen – eher seltenen Einsatzes des "IMSI-Catchers" ist auch nicht zu befürchten, dass die Regelung des § 100 i StPO die Bereitschaft zur Nutzung von Mobiltelefonen einschränkt. Im Übrigen sind die Ermittlungsbehörden bereits aus kriminaltaktischen Erwägungen und zur Erleichterung der Auswertung bemüht, den "IMSI-Catcher" nur im unmittelbaren Nahbereich der Zielperson einzusetzen, so dass die Anzahl der erfassten Mobiltelefone unbeteiligter Dritter und die dadurch verursachten Störungen möglichst gering gehalten werden. Ferner ist zu berücksichtigen, dass die IMSI- und IMEI-Nummern jeweils nur nacheinander erfasst werden können, so dass jeweils nur ein Funktelefon, nicht aber alle Telefone in einer Funkzelle zugleich von dem Einsatz betroffen sind.

83

bb) Sollte es dennoch zu einer kurzfristigen Versorgungslücke beim Erfassen der IMSI- oder IMEI-Nummer eines unbeteiligten Dritten kommen, so geht dieser Eingriff nicht über das Maß an Empfangs- und Sendestörungen hinaus, die im Mobilfunkbetrieb alltäglich auftreten. Dies gilt auch unter Berücksichtigung des Umstandes, dass ein Mobiltelefon nach Freigabe durch den "IMSI-Catcher" erst nach einer gewissen Zeit wieder zu seiner ursprünglichen Funkzelle zurückkehrt. Eine solche geringfügige Störung bei der Nutzung von Telekommunikationseinrichtungen ist jedenfalls angesichts der Bedürfnisse der Strafrechtspflege hinzunehmen (vgl. BVerfGE 100, 313 <388 ff.>; 107, 299 <316 ff.>).

84

4. Das Bundesministerium der Justiz hat mitgeteilt, seit längerem an einer Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen zu arbeiten, die die Vorschriften zur Telekommunikationsüberwachung und somit auch § 100 i StPO umfassen. Bei der Umsetzung dieser Vorschläge wird der Gesetzgeber die technischen Entwicklungen wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels aufmerksam beobachten und gegebenenfalls durch Rechtssetzung korrigierend eingreifen müssen (vgl. BVerfGE 112, 304 <320 f.>). Dabei wird zu prüfen sein, ob verfahrensrechtliche Vorkehrungen – wie etwa Benachrichtigungspflichten oder Rechtsschutzmöglichkeiten - zu erweitern sind, um den Grundrechtsschutz effektiv zu gewährleisten. Es stellt sich auch die Frage, ob und in welchem Umfang von einer neuerlichen Ausdehnung heimlicher Ermittlungsmethoden im Hinblick auf Grundrechtspositionen unbeteiligter Dritter Abstand zu nehmen ist.

85

Diese Entscheidung ist unanfechtbar.

Hassemer Di Fabio Landau