

Entwurf eines ... Gesetzes zur Änderung der Strafprozessordnung (Einführung einer Rechtsgrundlage zum verdeckten Zugriff auf informationstechnische Systeme)

A. Problem

Die Arbeit der Strafverfolgungsbehörden wird immer stärker von den neuen Technologien bestimmt. Internet, Miniaturisierung der Technologien, die nahezu grenzenlose Erhöhung des Speichervolumens und die Schnelligkeit der Informationsverarbeitung und -verbreitung haben sich auch Straftäter nutzbar gemacht. Islamistische Extremisten verbreiten im Internet ihre Propaganda oder organisieren Terroranschläge. Detaillierte Bombenbauanleitungen werden für jedermann zugänglich eingestellt. Einschlägige Foren und Tauschbörsen bieten einen Tummelplatz für Pädophile zur Vorbereitung des sexuellen Missbrauchs von Kindern sowie zur Verbreitung kinderpornografischer Darstellungen.

Der Trend zur Professionalisierung des Kommunikationsverhaltens der Beschuldigten ist unübersehbar und erschwert zunehmend die Strafverfolgung. Es steht zu befürchten, dass die frei zugänglichen, höchst wirksamen Kryptierungsverfahren, die Anonymisierung und Zugangssicherung (z. B. durch die Verschleierung von IP-Adressen oder die Verwendung von Passwörtern) die klassischen Ermittlungsinstrumentarien zur Beweissicherung künftig weitgehend ins Leere laufen lassen.

So reicht etwa die herkömmliche offene physische Beschlagnahme von Computern oder Festplatten gerade im Bereich des Terrorismus, aber auch bei anderen hoch konspirativen kriminellen Netzwerken, nicht mehr aus, um schwerwiegende Straftaten zu verfolgen. Die Beschlagnahme führt oftmals dazu, dass Mittäter gewarnt werden, da die strafprozessualen Maßnahmen offen durchgeführt werden.

Vor diesem Hintergrund ist im Einzelfall der Einsatz technischer Mittel zum verdeckten Zugriff auf informationstechnische Systeme notwendig, um Täter- und Tatstrukturen soweit aufklären zu können, dass offene Maßnahmen ohne Gefährdung des Ermittlungserfolges ermöglicht werden.

Mit Beschluss vom 31. Januar 2007 (NJW 2007, 930) hat der 3. Strafsenat des Bundesgerichtshofes den verdeckten Zugriff auf informationstechnische Systeme für un-

zulässig erklärt. Dies wurde damit begründet, dass keine entsprechende Rechtsgrundlage bestehe.

B. Lösung

Der Entwurf sieht die Schaffung einer Rechtsgrundlage für den verdeckten Zugriff auf informationstechnische Systeme vor. Er orientiert sich dabei an den Vorgaben des Bundesverfassungsgerichts insbesondere in seinem Urteil vom 27. Februar 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

C. Alternativen

Beibehaltung der bisherigen - unbefriedigenden - Rechtslage.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugaufwand

Keine.

2. Vollzugaufwand

Die Durchführung von verdeckten Zugriffen auf informationstechnische Systeme wird mit nicht konkret abschätzbaren zusätzlichen Kosten für den Bund und die Länder verbunden sein. Im Hinblick auf die zu erwartende geringe Zahl der Maßnahmen dürften die Mehrkosten für den Haushalt jedoch nicht ins Gewicht fallen.

E. Sonstige Kosten

Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

F. Bürokratiekosten

Es entstehen für die Wirtschaft und die Bürgerinnen und Bürger keine neuen Bürokratiekosten, jedoch für die Verwaltung. Für letztere wird eine neue Informationspflicht geschaffen. Die dadurch entstehenden Bürokratiekosten sind im Interesse einer effektiven Strafverfolgung nicht vermeidbar und geboten. Weniger belastende Alternativen zu den Informationspflichten bestehen nicht.

Entwurf eines ... Gesetzes zur Änderung der Strafprozessordnung

Vom ...

Der Bundestag hat folgendes Gesetz beschlossen:

Artikel 1 Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch ..., wird wie folgt geändert:

1. Nach § 100i wird folgender § 100k eingefügt:

"§ 100k

(1) Auch ohne Wissen des Betroffenen darf mit technischen Mitteln auf informationstechnische Systeme zugegriffen werden, um Zugangsdaten und gespeicherte Daten zu erheben, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat auch im Einzelfall besonders schwer wiegt und

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise - insbesondere durch eine Durchsuchung nach § 102, § 103 - unverhältnismäßig erschwert oder aussichtslos wäre.

(2) Straftaten im Sinne des Absatzes 1 Nr. 1 sind:

1. aus dem Strafgesetzbuch:

- a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80, 81, 82, nach den §§ 94, 95 Abs. 3 und § 96 Abs. 1, jeweils auch in Verbindung mit § 97b, sowie nach den §§ 97a, 98 Abs. 1 Satz 2, § 99 Abs. 2 und den §§ 100, 100a Abs. 4,
 - b) Bildung krimineller Vereinigungen nach § 129 Abs. 1 in Verbindung mit Abs. 4 Halbsatz 2 und Bildung terroristischer Vereinigungen nach § 129a Abs. 1, 2, 4, 5 Satz 1 Alternative 1, jeweils auch in Verbindung mit § 129b Abs. 1,
 - c) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen des § 176a Abs. 2 Nr. 2 oder Abs. 3, § 177 Abs. 2 Nr. 2 oder § 179 Abs. 5 Nr. 2,
 - d) Verbreitung, Erwerb und Besitz kinderpornografischer Schriften nach § 184b Abs. 1 bis 3,
 - e) Mord und Totschlag nach den §§ 211, 212,
 - f) Straftaten gegen die persönliche Freiheit in den Fällen der §§ 234, 234a Abs. 1, 2, §§ 239a, 239b und Menschenhandel zum Zweck der sexuellen Ausbeutung und zum Zweck der Ausbeutung der Arbeitskraft nach § 232 Abs. 3, Abs. 4 oder Abs. 5, § 233 Abs. 3, jeweils soweit es sich um Verbrechen handelt,
 - g) schwerer Raub und Raub mit Todesfolge nach § 250 Abs. 1 oder Abs. 2, § 251,
 - h) räuberische Erpressung nach § 255 und besonders schwerer Fall einer Erpressung nach § 253 unter den in § 253 Abs. 4 Satz 2 genannten Voraussetzungen,
2. aus dem Aufenthaltsgesetz:
- Einschleusen mit Todesfolge oder gewerbs- und bandenmäßiges Einschleusen nach § 97,
3. aus dem Betäubungsmittelgesetz:
- a) besonders schwerer Fall einer Straftat nach § 29 Abs. 1 Satz 1 Nr. 1, 5, 6, 10, 11 oder 13, Abs. 3 unter der in § 29 Abs. 3 Satz 2 Nr. 1 genannten Voraussetzung,
 - b) eine Straftat nach den §§ 29a, 30 Abs. 1 Nr. 1, 2, 4, § 30a,
4. aus dem Gesetz über die Kontrolle von Kriegswaffen:
- a) eine Straftat nach § 19 Abs. 2 oder § 20 Abs. 1, jeweils auch in Verbindung mit § 21,
 - b) besonders schwerer Fall einer Straftat nach § 22a Abs. 1 in Verbindung mit Abs. 2,
5. aus dem Völkerstrafgesetzbuch:
- a) Völkermord nach § 6,

b) Verbrechen gegen die Menschlichkeit nach § 7,

c) Kriegsverbrechen nach den §§ 8 bis 12,

6. aus dem Waffengesetz:

a) besonders schwerer Fall einer Straftat nach § 51 Abs. 1 in Verbindung mit Abs. 2,

b) besonders schwerer Fall einer Straftat nach § 52 Abs. 1 Nr. 1 in Verbindung mit Abs. 5.

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen, entgegengenommen haben, weitergeben oder weitergegeben haben oder dass der Beschuldigte ihre informationstechnischen Systeme benutzt oder benutzt hat. Die Maßnahme darf auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(4) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden, ist die Maßnahme unzulässig. Soweit dies informationstechnisch und ermittlungstechnisch möglich ist, ist durch geeignete Vorkehrungen sicherzustellen, dass die Erhebung von Daten unterbleibt, die dem Kernbereich der privaten Lebensgestaltung zuzurechnen sind. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 erlangt wurden, dürfen nicht verwertet werden, es sei denn, es bestehen Anhaltspunkte dafür, dass diese Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen. Aufzeichnungen über unverwertbare Erkenntnisse sind unverzüglich zu löschen oder bei Zweifeln dem für die Anordnung zuständigen Gericht zur Entscheidung über ihre Löschung vorzulegen. Die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen.

(5) Unter den Voraussetzungen des Absatz 1 dürfen technische Mittel auch eingesetzt werden, um

1. spezifische Kennungen zur Vorbereitung einer Maßnahme nach Absatz 1 sowie
2. den Standort eines informationstechnischen Systems zu ermitteln.

Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Nach Beendigung der Maßnahme sind diese unverzüglich zu löschen.

(6) Maßnahmen nach Absatz 1 und Absatz 5 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. § 100b Abs. 1 Sätze 4 und 5, Abs. 2 Satz 1, Abs. 4 Satz 1 sowie § 110 Abs. 1 gelten entsprechend. Neben den Angaben gemäß § 100b Abs. 2 Satz 2 Nr. 1 und 3 muss die Anordnung auch die Bezeichnung des informationstechnischen Systems enthalten. Maßnahmen nach Absatz 1 und Absatz 5 und insbesondere dadurch bedingte Veränderungen von Daten auf dem informationstechnischen System sind zu dokumentieren.

(7) Zur Durchführung von Maßnahmen nach Absatz 1 und Absatz 5 können Sachen verdeckt durchsucht sowie die Wohnung, in der sich das informationstechnische System befindet, ohne Einwilligung betreten und durchsucht werden. Für die Anordnung der Begleitmaßnahmen finden die für die Maßnahme nach Absatz 1 und Absatz 5 jeweils geltenden Vorschriften entsprechende Anwendung."

2. § 101 wird wie folgt geändert:

a) In Absatz 1 werden die Wörter „100c bis 100i“ durch die Wörter „100c bis 100k“ ersetzt.

b) Nach § 101 Abs. 4 Satz 1 Nr. 8 wird folgende Nr. 8a eingefügt:

"8a. des § 100k die Zielperson sowie die erheblich mitbetroffenen Personen,"

Artikel 2

Zitiergebot

Durch Artikel 1 dieses Gesetzes wird das Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) eingeschränkt.

Artikel 3
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeines

Die Arbeit der Strafverfolgungsbehörden wird immer stärker von den neuen Technologien bestimmt. Internet, Miniaturisierung der Technologien, die nahezu grenzenlose Erhöhung des Speichervolumens und die Schnelligkeit der Informationsverarbeitung und -verbreitung haben sich auch Straftäter nutzbar gemacht. Islamistische Extremisten verbreiten im Internet ihre Propaganda oder organisieren Terroranschläge. Detaillierte Bombenbauanleitungen werden für jedermann zugänglich eingestellt. Einschlägige Foren und Tauschbörsen bieten einen Tummelplatz für Pädophile zur Vorbereitung des sexuellen Missbrauchs von Kindern sowie zur Verbreitung kinderpornografischer Darstellungen.

Der Trend zur Professionalisierung des Kommunikationsverhaltens der Beschuldigten ist unübersehbar und erschwert zunehmend die Strafverfolgung. Deutlich zeigte sich dies bei den Ermittlungen, die schließlich zur Festnahme von Mitgliedern der „Islamic Jihad Union“ im September 2007 führten. Es gibt deutliche Hinweise, dass die Beschuldigten gezielt bezüglich ihres Kommunikationsverhaltens geschult wurden. Es ist davon auszugehen, dass die Kenntnisse der Täter hinsichtlich neuester Technologien bzw. Kommunikationsmittel weiter zunehmen werden. Hierbei steht zu befürchten, dass die frei zugänglichen, höchst wirksamen Kryptierungsverfahren, die Anonymisierung und Zugangssicherung (z. B. durch die Verschleierung von IP-Adressen oder die Verwendung von Passwörtern) die klassischen Ermittlungsinstrumentarien zur Informationserhebung und Beweissicherung künftig weitgehend ins Leere laufen lassen.

So reicht etwa die herkömmliche offene physische Beschlagnahme von Computern oder Festplatten gerade im Bereich des Terrorismus, aber auch bei anderen hoch konspirativen kriminellen Netzwerken, nicht mehr aus, um schwerwiegende Straftaten zu verfolgen. Die Beschlagnahme führt oftmals dazu, dass Mittäter gewarnt werden, da die strafprozessualen Maßnahmen offen durchgeführt werden. Vor allem im Zusammenhang mit terroristischen Tätern kann dies fatale Folgen haben. Darüber hinaus ist - anders als noch vor wenigen Jahren - aufgrund der fortschreitenden Technisierung nicht mehr gewährleistet, dass die Daten nach einer Beschlagnahme ausgewertet werden können. Insbesondere der Fortschritt auf dem Gebiet der Verschlüsselungstechniken bereitet zum Teil unüberwindbare Hindernisse

bei der Datenauswertung. Mit fortschreitender technischer Entwicklung wird sich diese Problematik noch ganz erheblich verschärfen.

Vor diesem Hintergrund ist im Einzelfall der Einsatz technischer Mittel zum verdeckten Zugriff auf informationstechnische Systeme notwendig, um Täter- und Tatstrukturen soweit aufklären zu können, dass offene Maßnahmen ohne Gefährdung des Ermittlungserfolges ermöglicht werden.

Das Bundesverfassungsgericht anerkennt in diesem Zusammenhang die Notwendigkeit staatlichen Handelns. In seinem Urteil zum verdeckten Zugriff auf informationstechnische Systeme vom 27. Februar 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, führt das Gericht in Absatz-Nr. 220 aus: „Die Sicherheit des Staates als verfasster Friedens- und Ordnungsmacht und die von ihm zu gewährleistende Sicherheit der Bevölkerung vor Gefahren für Leib, Leben und Freiheit sind Verfassungswerte, die mit anderen hochwertigen Gütern im gleichen Rang stehen (vgl. BVerfGE 49, 24 <56 f.>; 115, 320 <346>). Die Schutzpflicht findet ihren Grund sowohl in Art. 2 Abs. 2 Satz 1 als auch in Art. 1 Abs. 1 Satz 2 GG (vgl. BVerfGE 115, 118 <152>). Der Staat kommt seinen verfassungsrechtlichen Aufgaben nach, indem er Gefahren durch terroristische oder andere Bestrebungen entgegen tritt. Die vermehrte Nutzung elektronischer oder digitaler Kommunikationsmittel und deren Vordringen in nahezu alle Lebensbereiche erschwert es der Verfassungsschutzbehörde, ihre Aufgaben wirkungsvoll wahrzunehmen. Auch extremistischen und terroristischen Bestrebungen bietet die moderne Informationstechnik zahlreiche Möglichkeiten zur Anbahnung und Pflege von Kontakten sowie zur Planung und Vorbereitung, aber auch Durchführung von Straftaten. Maßnahmen des Gesetzgebers, die informationstechnische Mittel für staatliche Ermittlungen erschließen, sind insbesondere vor dem Hintergrund der Verlagerung herkömmlicher Kommunikationsformen hin zum elektronischen Nachrichtenverkehr und der Möglichkeiten zur Verschlüsselung oder Verschleierung von Dateien zu sehen (vgl. zur Strafverfolgung BVerfGE 115, 166 <193>).“

Der verdeckte Einsatz von technischen Mitteln, um auf informationstechnische Systeme zugreifen und Zugangsdaten und gespeicherte Daten erheben zu können, zählt angesichts des rasanten technischen Fortschritts zu den unverzichtbaren Instrumenten der Strafverfolgung. Den Strafverfolgungsbehörden muss daher auch in Zukunft das notwendige Instrumentarium zur Verfügung stehen, um in hoch konspirative kriminelle Netze eindringen zu können und Straftaten gegen überragend wichtige Rechtsgüter effektiv verfolgen zu können. Andernfalls besteht aufgrund des schnellen Fortschrittes in der Informationstechnologie und der steigenden Konspirativität der Täter die Gefahr unverantwortbarer Ermittlungslücken und de facto rechtsfreier Räume.

Mit Beschluss vom 31. Januar 2007 (NJW 2007, 930) hat der 3. Strafsenat des Bundesgerichtshofes den verdeckten Zugriff auf informationstechnische Systeme (entgegen einigen früheren gerichtlichen Entscheidungen) für unzulässig erklärt. Dies wurde damit begründet, dass keine entsprechende Rechtsgrundlage bestehe. Nach der Entscheidung ist die verdeckte Online-Durchsuchung insbesondere nicht durch § 102 StPO (Durchsuchung beim Verdächtigen) gedeckt, weil die Durchsuchung in der Strafprozessordnung als eine offen durchzuführende Ermittlungsmaßnahme geregelt sei. Dies ergebe sich zum einen aus mehreren Vorschriften des Durchsuchungsrechts zu Gunsten des Beschuldigten - Anwesenheitsrecht (§ 106 Abs. 1 Satz 1 StPO) und Zuziehung von Zeugen (§ 105 Abs. 2, § 106 Abs. 1 Satz 2 StPO) -, deren Befolgung als zwingendes Recht nicht zur Disposition der Ermittlungsorgane stehe. Zum anderen folge dies aus einem Vergleich mit den Ermittlungsmaßnahmen, die - wie die Überwachung der Telekommunikation (§§ 100a, b StPO) oder die Wohnraumüberwachung (§§ 100c, d StPO) - ohne Wissen des Betroffenen durchgeführt werden könnten, für die aber deutlich höhere formelle und materielle Anforderungen an die Anordnung und Durchführung bestünden.

Mit der Vorschrift des § 100k StPO-E wird der verdeckte Zugriff auf informationstechnische Systeme nunmehr auf eine gesetzliche Grundlage gestellt. Der Entwurf orientiert sich dabei an den verfassungsrechtlichen Vorgaben, die das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008, Az.: 1 BvR 370/07, 1 BvR 595/07, für den Schutz des vom allgemeinen Persönlichkeitsrecht nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG umfassten Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgestellt hat. Er berücksichtigt ferner die vom Bundesverfassungsgericht bereits früher für Maßnahmen der verdeckten Datenerhebung aufgestellten Maßstäbe, insbesondere in den Entscheidungen vom 3. März 2004 zur akustischen Wohnraumüberwachung, Az. 1 BvR 2378/98, 1 BvR 1084/99, und zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz, Az. 1 BvF 3/92, sowie im Urteil vom 27. Juli 2005 zum niedersächsischen Sicherheits- und Ordnungsgesetz, Az.: 1 BvR 668/04.

B.

Zu den einzelnen Bestimmungen

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Artikel 1 Nr. 1 (§ 100k StPO)

Zu Absatz 1

Ziel der Maßnahme ist der verdeckte Zugriff auf informationstechnische Systeme zur Erhebung von Daten, soweit dies für die Verfolgung schwerwiegender Straftaten erforderlich ist.

Zielobjekt der Maßnahme sind stets informationstechnische Systeme. Nach der Definition des Bundesverfassungsgerichts (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 202 f.) sind darunter Systeme zu verstehen, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. Eine solche Möglichkeit besteht etwa beim Zugriff auf Personalcomputer, einerlei ob sie fest installiert oder mobil betrieben werden.“

Auch solche Mobiltelefone und elektronische Terminkalender, die über einen großen Funktionsumfang verfügen und personenbezogene Daten vielfältiger Art erfassen und speichern können, fallen darunter.

Der Zugriff auf informationstechnische Systeme bedeutet, dass die notwendigen technischen Maßnahmen ergriffen werden, um eine Datenerhebung zu ermöglichen. Die Regelung unterscheidet zunächst zwischen Zugangsdaten und gespeicherten Daten. Zugangsdaten sind meist nicht im informationstechnischen System abgelegt und dienen als Schlüssel, um den Zugang zu den gespeicherten Daten zu eröffnen. Zugangsdaten sind insbesondere Benutzerkennungen, Pass- und Kennwörter; aber auch die von einem informationstechnischen System geforderte Authentifizierung mittels Fingerprint wäre hiervon erfasst. Die Regelung ermöglicht den Strafverfolgungsbehörden damit auch die Erfassung von Tastatureingaben, um dann später mit Hilfe des erhobenen Kennwortes auf kryptierte oder anderweitig vor Zugriff besonders geschützte Daten zugreifen zu können. Eine gesetzliche Regelung ist erforderlich, weil das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität auch vor Datenerhebungen mit Mitteln schützt, die zwar technisch von den Datenverarbeitungsvorgängen des betroffenen informationstechnischen Systems unabhängig sind, aber diese Datenverarbeitungsvorgänge zum Gegenstand haben. So liegt es etwa beim Einsatz von sogenannten Hardware-Keyloggern oder bei einer Messung der elektromagnetischen Abstrahlung von Bildschirm oder Tastatur (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 205). Der Einsatz von Keyloggern kann insbesondere notwendig sein, um später entweder die eigentlich zur Strafverfolgung erforderlichen Daten im Rahmen einer verdeckten Maßnahme zu erheben oder im Wege der offenen Sicherstellung die Datenträger, die gegen den Zugriff Dritter besonders gesichert sind, in Gewahrsam zu nehmen und aus-

zuwerten. Angesichts der zunehmenden Verbreitung von im Internet als Freeware herunterladbaren Kryptier- bzw. Verschlüsselungsprogrammen, ermöglicht die verdeckte Erhebung von Zugangsdaten eine nachfolgende offene Beschlagnahme und Auswertung des Speichermediums. Obwohl die Erfassung von Zugangsdaten gegenüber der Erhebung von gespeicherten Daten regelmäßig die weniger eingriffsintensive Maßnahme darstellen wird, gelten auch hier die gleich strengen Voraussetzungen.

Gespeicherte Daten sind sowohl die im Arbeitsspeicher gehaltenen als auch die temporär oder dauerhaft auf den Speichermedien des Systems abgelegten Daten (vgl. Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 205).

Bei den Daten darf es sich um keine Telekommunikationsdaten handeln. Soweit sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt, trifft § 100a StPO eine Sonderregelung. Entsprechendes gilt für die Wohnraumüberwachung. Soweit eine Überwachungsmaßnahme darauf abzielt, keine Zugangsdaten eines informationstechnischen Systems oder darin gespeicherte Daten, sondern Lebensäußerungen aus einer Wohnung zu erheben, ist § 100c StPO spezieller. Umgekehrt greift § 100k StPO-E auch dann ein, wenn sich das informationstechnische System in einer Wohnung im Sinne von Art. 13 GG befindet.

Eingriffshandlung nach Absatz 1 ist das Erheben von Daten. Das Erheben von Zugangsdaten betrifft insbesondere die Erhebung von Benutzerkennungen und Passwörtern, nicht aber schon die Erhebung von besonders gesicherten Daten. Das Erheben von gespeicherten Daten umfasst die bloße Sichtung, aber auch das Kopieren von Datenbeständen unter Belassung der Datenbestände auf dem Zielsystem.

Nicht erfasst von der Befugnis sind allgemeine Recherchen im Internet durch die Strafverfolgungsbehörden, auch wenn Ermittlungspersonen nicht als solche und unter ihrem eigenen Namen auftreten. Hier liegt in der Regel kein Grundrechtseingriff vor (vgl. auch insoweit Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 311), sodass es keiner Rechtsgrundlage bedarf.

Besondere Bedeutung kommt der ausdrücklich im Gesetz normierten Voraussetzung zu, dass die Tat auch im ganz konkreten Einzelfall besonders schwer wiegen muss (Absatz 1 Nr. 2). Auch durch sie wird im Einzelfall der konkrete Bezug zum überragend wichtigen Rechtsgut hergestellt. Einzubeziehen ist jeweils auch die Eingriffsintensität. So bedeutet beispielsweise die verdeckte Erhebung eines Passwortes, mit dessen Hilfe nach einer sich anschlie-

ßenden offenen Durchsuchung und Beschlagnahme des Computers die Möglichkeit zur Auswertung eröffnet wird, im Hinblick auf das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme im Vergleich zu einer verdeckten Erhebung von auf dem informationstechnischen System gespeicherten Daten den weniger intensiven Eingriff.

Die in Absatz 1 Nr. 3 zusätzlich genannten Voraussetzungen, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise aussichtslos oder unverhältnismäßig erschwert wäre, betonen die Subsidiarität der Maßnahme. Insoweit wird ergänzend die Subsidiarität zur offenen Durchsuchung klargestellt.

Zu Absatz 2

Der Straftatenkatalog für den verdeckten Zugriff auf informationstechnische Systeme lehnt sich an den für eine Wohnraumüberwachung (§ 100c StPO) an.

Das Bundesverfassungsgericht führt in seiner Entscheidung vom 27. Februar 2008 ausdrücklich aus, dass das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht schrankenlos sei und Eingriffe auch zur Strafverfolgung gerechtfertigt sein können (Absatz-Nr. 207). Nähere Ausführungen zu den Voraussetzungen hierfür fehlen in der Entscheidung. Angesichts der hohen Eingriffsschwellen im präventiven Bereich (nur bei drohenden Gefahren für Leib, Leben und Freiheit zulässig sowie bei Bedrohungen, die den Bestand des Staates oder die Grundlagen der menschlichen Existenz berühren) muss der Straftatenkatalog eng begrenzt sein und sich auf diese Rechtsgüter beziehen.

Der Straftatenkatalog des § 100c StPO, der sich auf einen Grundrechtseingriff ähnlicher Eingriffstiefe bezieht, ist wegen der verfassungsrechtlichen Vorgaben in Art. 13 Abs. 3 GG auf besonders schwere Straftaten beschränkt. Auf der Basis dieses Katalogs ist in Absatz 2 ein eigener Katalog für den verdeckten Zugriff auf informationstechnische Systeme zusammengestellt, der diejenigen Delikte herausgreift, die sich auf die Rechtsgüter Leib, Leben und Freiheit sowie auf den Schutz des Bestands des Staates bzw. der Grundlagen der menschlichen Existenz beziehen.

Über den Katalog des § 100c StPO hinaus sind § 184b Abs. 1 und 2 StGB aufgenommen. Diese Tatbestände weisen zwar nur einen Strafrahmen bis zu fünf Jahren auf. Es handelt sich jedoch um besonders gravierende Delikte, denen in der Regel ein realer sexueller Miss-

brauch eines Kindes zugrunde liegt. Zudem handelt es sich um typische Delikte der Internetkriminalität, bei denen gerade die Verbreitung mit Hilfe von informationstechnischen Systemen erfolgt.

Zu Absatz 3

Absatz 3 regelt den Adressaten der Maßnahme. Neben dem Beschuldigten kommen auch Dritte als Adressaten in Betracht, wenn auf der Grundlage von bestimmten Tatsachen die begründete Annahme besteht, dass es sich um Kontaktpersonen handelt oder um Personen, die ihre informationstechnischen Systeme dem Beschuldigten in der Vergangenheit zur Verfügung gestellt haben oder zur Verfügung stellen.

Zu Absatz 4

Aufgrund der Rechtsprechung des Bundesverfassungsgerichts (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 280) müssen Regelungen aufgenommen werden, die den Kernbereich privater Lebensgestaltung von verdeckten Zugriffen auf informationstechnische Systeme freihalten. Insoweit sieht die Entscheidung des Bundesverfassungsgerichts ein zweistufiges Schutzkonzept vor.

Durch Absatz 4 Sätze 1 und 2 wird auf der ersten Stufe darauf hingewirkt, dass soweit dies informationstechnisch und ermittlungstechnisch möglich ist, mittels geeigneter Vorkehrungen sicherzustellen ist, dass bereits die Erhebung von kernbereichsrelevanten Daten unterbleibt. Dabei sind entsprechend den Ausführungen des Bundesverfassungsgerichts „verfügbare“ informationstechnische Sicherungen einzusetzen (vgl. Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 281). Satz 2 steht unter dem Vorbehalt des informationstechnisch und ermittlungstechnisch Möglichen, indem die Sicherstellung in der Erhebungsphase voraussetzt, dass geeignete Vorkehrungen vorhanden und einsetzbar sind. Auch das Bundesverfassungsgericht stellt in seiner Entscheidung vom 27. Februar 2008 fest, dass es bei einem heimlichen Zugriff auf ein informationstechnisches System praktisch unvermeidbar sei, Informationen zur Kenntnis zu nehmen, bevor ihr Kernbereichsbezug bewertet werden kann (Absatz-Nr. 277). Weiter heißt es in der Entscheidung, dass „technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten [...] nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig [arbeiten], dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte“ (Absatz-Nr. 278).

In der zweiten Stufe ist ein Verwertungsverbot für dennoch erhobene Kernbereichsdaten vorgesehen. Eine Ausnahme besteht jedoch in den Fällen, in denen Anhaltspunkte bestehen, dass kernbereichsrelevante Daten dem Zweck der Herbeiführung eines Erhebungsverbots dienen sollen. Das Bundesverfassungsgericht hat anerkannt, dass von dem grundsätzlichen Erhebungsverbot kernbereichsrelevanter Daten eine Ausnahme zu machen ist, wenn konkrete Anhaltspunkte dafür bestehen, dass kernbereichsbezogene Kommunikationsinhalte mit Inhalten verknüpft werden, die dem Ermittlungsziel unterfallen, um eine Überwachung zu verhindern (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 281).

Entscheidende Bedeutung für den Schutz des Betroffenen hat „die Durchsicht der erhobenen Daten auf kernbereichsrelevante Inhalte [...], für die ein geeignetes Verfahren vorzusehen ist, das den Belangen des Betroffenen hinreichend Rechnung trägt“ (Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 283). Ein solches geeignetes Verfahren wird in Absatz 4 Satz 4 geregelt. Die durch den Zugriff auf informationstechnische Systeme erlangten Daten sind unverzüglich zu sichten. Bestehen Anhaltspunkte, dass kernbereichsrelevante Daten erhoben wurden, so sind diese entweder unverzüglich zu löschen oder bei Zweifeln dem für die Anordnung der Maßnahme zuständigen Richter vorzulegen; dieser entscheidet dann über die Löschung. Absatz 4 Satz 5 ordnet die Dokumentation der Löschung an.

Für den Schutz von Berufsgeheimnisträgern gilt ebenso wie bei anderen verdeckten Ermittlungsmaßnahmen § 160a StPO. Einer gesonderten Regelung für den verdeckten Zugriff auf informationstechnische Systeme bedarf es nicht.

Zu Absatz 5

Im Unterschied zum Zugriff auf informationstechnische Systeme zur Erhebung von Zugangsdaten oder gespeicherten Daten normiert Absatz 5 die Befugnis zum Einsatz von technischen Mitteln zur Identifikation und Lokalisation von informationstechnischen Systemen. Diese Regelung ist angesichts der Entwicklungen auf dem Gebiet der Informationstechnik erforderlich, da bei der Begehung von schwerwiegenden Straftaten im Sinne von Absatz 2 zunehmend informationstechnische Systeme eingesetzt werden, deren spezifische Kennungen und Standort den Strafverfolgungsbehörden nicht bekannt sind. Eine Spezifizierung der informationstechnischen Systeme ist allerdings im Regelfall Voraussetzung für die Durchführung einer Maßnahme nach Absatz 1. Gleiches gilt für die Bestimmung des Standorts eines informationstechnischen Systems. Der Einsatz von Geräten, wie etwa des sog.

„WLAN-Catchers“ zur Bestimmung von spezifischen Kennungen bzw. des Standortes eines informationstechnischen Systems wird an die strengen Voraussetzungen des Absatz 1 geknüpft, da er in der Regel zur Vorbereitung einer der dort genannten Maßnahmen dient. Soweit aus technischen Gründen unvermeidbar Daten Dritter erhoben werden, sind diese unverzüglich zu löschen.

Zu Absatz 6

Angesichts der Grundrechtsintensität ist die Schaffung eines Richtervorbehalts erforderlich (vgl. hierzu auch Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 257 ff.). Eine Eilzuständigkeit der Staatsanwaltschaft bei Gefahr in Verzug vergleichbar der Zuständigkeitsregelung bei der Telekommunikationsüberwachung in § 100b Abs. 1 Satz 1 StPO erscheint wegen des zeitlichen Vorlaufs für die technische Vorbereitung einer solchen Maßnahme entbehrlich.

Die richterliche Anordnung ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Dies ergibt sich aus dem Verweis auf § 100b Abs. 1 Sätze 4 und 5 StPO. Die zulässige Höchstdauer für eine Anordnung trägt dem Umstand Rechnung, dass in der Praxis die Durchführung eines verdeckten Zugriffs auf informationstechnische Systeme regelmäßig langwieriger Vorbereitungen bedarf. Eine kürzere Anordnungshöchstdauer würde in diesen Fällen die Beantragung einer erneuten Anordnung erfordern, bevor mit der eigentlichen Maßnahme begonnen worden ist. Da es sich um eine Bestimmung der Höchstdauer handelt, kann das anordnende Gericht je nach Lage des Einzelfalls die Maßnahme auch für eine kürzere Frist anordnen. Die Vorschrift erlaubt nicht nur einen einmaligen Zugriff auf das informationstechnische System. Vielmehr kann innerhalb der Anordnungsfrist auch mehrfach zugegriffen werden.

Für Form und Inhalt der Anordnung wird auf § 100b Abs. 2 StPO verwiesen (soweit diese Vorschrift nicht spezielle Merkmale einer Telekommunikationsüberwachung betrifft), für die Frage der Beendigung der Maßnahme nach Wegfall der Voraussetzungen auf § 100b Abs. 4 Satz 1 StPO. Anordnungen sind danach schriftlich abzufassen und zu begründen. Die Anordnung muss auch die Bezeichnung des informationstechnischen Systems enthalten. Name und Anschrift des Betroffenen sind nur anzugeben, soweit dies möglich ist. Es gibt durchaus Fallkonstellationen, bei denen die Strafverfolgungsbehörden den Maßnahmedressaten nur über das informationstechnische System ermitteln können.

Hinsichtlich der Durchsicht der Daten, auf die zugegriffen wurde, wird auf § 110 StPO verwiesen, der nach herrschender Meinung bereits bisher auch auf die Durchsicht von Daten anwendbar war, die im Rahmen einer konventionellen Durchsuchung beschlagnahmt wurden. Demnach steht die Durchsicht der Staatsanwaltschaft und auf deren Anordnung ihren Ermittlungspersonen zu. Dies entspricht dem Verfahren bei der Beschlagnahme von Festplatten im Rahmen einer konventionellen Durchsuchung.

Der verdeckte Zugriff auf informationstechnische Systeme kann zu Datenveränderungen auf dem Zielsystem führen. Daher ist in Absatz 6 Satz 3 vorgesehen, den ursprünglichen Zustand des informationstechnischen Systems sowie die Auswirkungen der Maßnahmen der Strafverfolgungsbehörden umfassend zu dokumentieren. Durch die Dokumentation der einzelnen Schritte der Maßnahme wird die Nachvollziehbarkeit aller getroffenen Maßnahmen gewährleistet. Die Interessen der Betroffenen werden dadurch insbesondere im Hinblick auf die spätere Beweiswürdigung im weiteren Verfahren abgesichert.

Eine gesonderte Regelung zur Verwendung der erlangten Daten für andere Strafverfahren oder für präventive Zwecke ist im Hinblick auf § 477 Abs. 2 Satz 2 und 3 StPO nicht erforderlich.

Zu Absatz 7

Absatz 7 enthält die Ermächtigung zur Durchführung notwendiger Begleitmaßnahmen. Die „Hauptmaßnahmen“ wären ohne die notwendigen Begleitmaßnahmen nach Satz 1 (Durchsuchung von Sachen, Betreten und Durchsuchung der Wohnung, in der sich das informationstechnische System befindet) vielfach gar nicht möglich. Zu diesen Begleitmaßnahmen zählen etwa regelmäßig das Betreten der Wohnung, die heimliche Durchsuchung der Wohnung zur Auffindung z.B. eines Notebooks und das Anbringen von Hardwarekomponenten (z.B. von Hardware-Keyloggern zur Erfassung von Passwörtern verschlüsselter Dateien) oder das Einbringen spezifischer Software für den Zugriff auf das informationstechnische System.

Insoweit besteht ein Bedürfnis für eine ausdrückliche gesetzliche Regelung. Zwar sind nach jedenfalls herrschender Meinung notwendige Beeinträchtigungen des Betroffenen durch typischerweise mit der Maßnahme verbundene Vorbereitungs- und Begleitmaßnahmen durch die Befugnisnorm gedeckt (Meyer-Goßner, Strafprozessordnung, 50. Auflage, § 100f Rdnr. 7). Für die oben beschriebenen Begleitmaßnahmen wird jedoch unter Umständen insbesondere in das Grundrecht auf Unverletzlichkeit der Wohnung (Art. 13 GG) eingegrif-

fen. Hierfür muss eine eigenständige Rechtsgrundlage geschaffen werden (vgl. Urteil des Bundesverfassungsgerichts vom 27. Februar 2008, a.a.O., Absatz-Nr. 193).

Art. 13 Abs. 2 GG lässt ein heimliches Eindringen in die Wohnung zur Durchführung von Begleitmaßnahmen zu. Dass die Offenheit Wesensmerkmal einer Durchsuchung im Sinne dieser Vorschrift ist, lässt sich der Verfassungsrechtsprechung nicht entnehmen, auch nicht der oben angeführten Fundstelle im Urteil des Bundesverfassungsgerichts vom 27. Februar 2008. Unter die insoweit gebräuchliche verfassungsrechtliche Definition der Durchsuchung (Tätigkeiten, die von einem ziel- und zweckgerichteten Suchen staatlicher Organe in einer Wohnung nach etwas Verborgenen geprägt sind; vgl. BVerfGE 51, 97, 106f; 75, 318, 327; vgl. auch Sachs, GG, 3. Aufl., Art. 13 Rn. 27) kann auch die heimliche Durchsuchung subsumiert werden. Dass der Bundesgerichtshof in seinem Beschluss vom 31. Januar 2007 (NJW 2007, 930) die verdeckte Online-Durchsuchung insbesondere nicht durch § 102 StPO gedeckt sah, weil die Durchsuchung in der Strafprozessordnung als eine offen durchzuführende Ermittlungsmaßnahme geregelt sei, steht dieser Beurteilung nicht entgegen, da sich der BGH zur Begründung nur auf formelle Vorschriften der StPO berief.

Allerdings ist eine dem Betroffenen verheimlichte Durchsuchung ein schwerwiegenderer Grundrechtseingriff als eine Durchsuchung, die mit Wissen des Betroffenen durchgeführt wird. Der Entwurf berücksichtigt dies.

Für die Anordnung der Begleitmaßnahmen gelten nach Satz 2 die gleichen Vorschriften wie für die Hauptmaßnahme. Der Straftatenkatalog ist zu beachten, es besteht zur verfahrensmäßigen Absicherung der Rechte des Betroffenen ein Richtervorbehalt und in der richterlichen Anordnung sind Art, Umfang und Dauer der Maßnahme genau zu bestimmen. Auch für die Unterrichtung gelten dieselben Regeln wie bei der Hauptmaßnahme.

Zu Artikel 1 Nr. 2 (§ 101 StPO)

Die Änderung von § 101 Abs. 1 soll klarstellen, dass die Regelungen dieser Vorschrift (insbesondere Kennzeichnungs-, Löschungs- und Benachrichtigungspflichten) auch für den verdeckten Zugriff auf informationstechnische Systeme gelten.

Die Benachrichtigungspflicht nach Absatz 4 Satz 1 Nr. 8a erfasst – ähnlich wie Nr. 5 - die Adressaten der Maßnahme und die erheblich mitbetroffenen Personen.

Zu Artikel 2 (Zitiergebot)

Nach dem Zitiergebot des Art. 19 Abs. 1 Satz 2 GG kann ein Gesetz nur dann verfassungsrechtlich gerechtfertigt sein, wenn es das eingeschränkte Grundrecht unter Angabe des Artikels nennt. Da das Grundrecht auf Unverletzlichkeit der Wohnung in Art. 13 GG unter einen ausdrücklichen Gesetzesvorbehalt gestellt wird, ist ein Hinweis auf dessen Einschränkung erforderlich.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.