Seminar: Strafprozessuale Grundrechtseingriffe

Die Anforderung von Verbindungsdaten der Telekommunikation, §§ 100g, 100h StPO

A. Einleitung

I. Historie, Überblick

Die Paragraphen 100g und 100h der Strafprozessordnung sind durch das Gesetz zur Änderung der StPO vom 20. Dezember 2001[1] eingefügt worden. Sie lösen den § 12 Fernmeldeanlagengesetz[2] (FAG) ab, der 1928 in Kraft trat und in den letzten Jahren mehrfach verlängert wurde[3], u.a. nach dem erfolglosen Entwurf eines § 99a StPO[4].

Der alte § 12 FAG bezog sich auf Daten, die die „Damen vom Amt" handschriftlich, auf Grund der von ihnen vermittelten Verbindung, festhielten[5]. Bei der späteren automatisch-analogen Vermittlung fielen keine (Verbindungs-)Daten an, sodass der § 12 FAG ein „Schattendasein" führte[6].

Seit Einführung der digitalen Vermittlungstechnik zu Beginn der 1990er Jahre wird zu jeder Telekommunikation verbindungserforderlich automatisch ein Datensatz erzeugt, der die beteiligten Anschlüsse, Rufnummer, Datum, Uhrzeit, Dauer und Ort der Kommunikation enthält. Aus den ca. 100 Milliarden Verbindungen in Deutschland pro Jahr lassen sich damit die Telekommunikationsbeziehungen einer ganzen Gesellschaft rekonstruieren[7].

Eine Neuregelung der auf Grund der technischen Entwicklung verfassungsrechtlich bedenklich gewordenen Auskunftserteilung wurde nötig.

Bereits im Herbst 2000 erhielt das Institut für deutsches und europäisches Strafprozessrecht und Polizeirecht an der Mannheimer Fakultät für Rechtswissenschaften unter Leitung der Professoren Wolter und Schenke vom Bundesministerium der Justiz den Auftrag, einen Gesetzesvorschlag für eine Nachfolgeregelung des § 12 FAG zu erarbeiten[8].

---

[1] BGBl. 2002 I, S. 3879; Wollweber, NJW 2002, 1554.

[2] Gesetzestext des § 8c des Gesetzes zur Änderung des Telegraphengesetzes v. 3.12.1927; RGBl. I, S. 331, 332; wortgleich neu verkündet als § 12 FAG am 14.1.1928, RGBl. I, S. 8; Welp, Überwachung und Kontrolle, S. 21; Thomas Königshofen, Konzerndatenschutzbeauftragter der Dt. Telekom AG, 05.10.2000: http://bund.de/information/vortrag6pp.

[3] Begleitgesetz zum Telekommunikationsgesetz vom 17.12.1997, BGBl. I, S. 3108: bis 31.12.99; Art. 4 Nr. 2 des Gesetzes [...] zur Änderung des Gesetzes über Fernmeldeanlagen vom 20.12.99, BGBl. I, S. 2491: bis 31.12.2001.

[4] BT-Drs. 13/8776, S. 31 ff.

[5] Vgl. Welp, GA 2002, 535 (536) m.w.N.; „Wer hat wann wie lange mit wem gesprochen?"

[6] Paeffgen, in Roxin-FS, Überlegungen zu einer Reform des Rechts der Überwachung der Kommunikation, S. 413 (416).

[7] Welp, GA 2002, 535 (536).

[8] Hilger, GA 2002, 228.

Ein Vorschlag des „Arbeitskreis Strafprozessrecht und Polizeirecht“ (ASP) wurde größtenteils als Regierungsentwurf in den Bundestag eingebracht[9].

Auf Grund der Eilbedürftigkeit einer neuen Regelung (§ 12 FAG befristet bis 31.12. 2001) wurde auf die Anrufung des Vermittlungsausschusses durch die Reformgegner verzichtet[10].

Die neu eingefügten Normen sind bis zum 31.12.2004 befristet, da eine harmonisierte gesetzliche Gesamtregelung strafprozessualer Grundrechtseingriffe auf Grund laufender Forschungsvorhaben geplant ist[11].

Die Anforderung von Telekommunikationsverbindungsdaten ist ein strafprozessualer Grundrechtseingriff[12], da mit der Anordnung in das Fernmeldegeheimnis, Artikel 10 Abs. 1 Grundgesetz, eingegriffen wird. Des Weiteren kann das Grundrecht auf informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG, betroffen sein[13].

Nach einer Übersicht und einigen Begriffsdefinitionen wird auf den Gegenstand der Auskunftspflicht, die materiellen Eingriffsvoraussetzungen und den Anwendungsbereich der §§ 100g, h StPO einzugehen sein.

II. Allgemeines

§ 100g I 1 StPO beinhaltet die Pflicht zur Erteilung von Auskunft über TK-Verbindungsdaten[14]. Hilfreich ist die genaue Abgrenzung der Begriffe Telekommunikation, TK-Inhalte und TK-Verbindungsdaten.

1. Definitionen

Das Telekommunikationsgesetz (TKG) vom 25.07.1996[15] enthält in § 3 gesetzliche Definitionen, die Anhaltspunkte für eine Konkretisierung des Fernmeldegeheimnisses geben können.

Telekommunikation ist nach § 3 Nr. 16 TKG

der „technische Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art [...] mittels *Telekommunikationsanlagen*“.

Unter ***Anlagen der TK*** versteht man

---

[9] BT-Drs. 14/7008, S. 1 ff.

[10] BT-Drs. 14/7679, S. 6, 7 f.

[11] Max-Planck-Institut (MPI) für ausländisches und internationales Strafrecht, Freiburg: rechtstatsächliche Untersuchung zur Rechtswirklichkeit und Effizienz der Überwachungsvorschriften, www.iuscrim.mpg.de/forsch/krim/albrecht.html; Hilger, GA 2002, 228 (230, 231).

[12] Begriff: Amelung, JZ 1987, 737 (738).

[13] BVerfGE 67, 157 (171); 100, 313 (358).

[14] Dazu gehören nicht Teledienstenutzungsdaten iSd. Teledieste- (TDG) und Teledienstedatenschutzgesetz (TDDSG) (z. B. Daten vom Besuch einer Homepage); BT-Drs. 14/7679, S. 7; SK/StPO/Wolter, § 100g, Rn 10; anders aber §§ 8 III BVerfSchG, 10 III MADG, 8 III a BNDG.

[15] BGBl. 1996 I, S. 1120; geändert durch BegleitG zum TKG vom 17.12.1997; BGBl. I, 3108.

„technische Einrichtungen [...], die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übermitteln, empfangen [...] können." (§ 3 Nr. 17 TKG)

Telekommunikations-Dienstleistungen sind das „gewerbliche Angebot vom Telekommunikation"[16].

Geschäftsmäßiges Erbringen von Telekommunikations-Diensten „ist das nachhaltige Angebot von Übertragungswegen für Dritte [...][17].

Die Telekommunikations-Datenschutzverordnung[18] (TDSV) regelt den Schutz personenbezogener Daten (§ 1 I TDSV), die durch Telekommunikationsunternehmen erhoben, verarbeitet oder genutzt werden. Danach sind ***Bestandsdaten*** „personenbezogene Daten eines an der Telekommunikation Beteiligten, die erhoben werden, um ein Vertragsverhältnis über Telekommunikationsdienste [...] mit dem Dienstesanbieter zu begründen oder zu ändern"[19]. Name und Anschrift eines TK-Teilnehmers sind solche Bestands- bzw. Vertragsdaten.

§ 2 Nr. 4 TDSV definiert ***Verbindungsdaten*** als „personenbezogene Daten [...], die bei der Bereitstellung und Erbringung von TK-Diensten erhoben werden", z.B. Beginn und Ende einer Telekommunikation oder die Kennung des Standortes.

Die Telekommunikations-Überwachungsverordnung[20] (TKÜV) regelt die technische und organisatorische Umsetzung von Telekommunikationsüberwachungsmaßnahmen i.V.m. der Ermächtigungsgrundlage § 88 TKG.

<table>
<tr><td colspan="3">Telekommunikation, § 3 Nr. 16 TKG</td></tr>
<tr><td><u>Bestandsdaten</u>
§ 2 Nr. 3 TDSV
Name, Adresse, Rufnummer</td><td><u>Verbindungsdaten</u>
§ 2 Nr. 4 TDSV, § 100g III StPO
angerufene Nummer,
Verbindungsdauer</td><td><u>Inhaltsdaten</u>
ausgetauschte Nachrichten, z.B.:
Gesprächsinhalte, Faxe, E-Mails</td></tr>
<tr><td></td><td colspan="2">Art. 10 I GG</td></tr>
<tr><td colspan="3">Art. 2 I, 1 I GG</td></tr>
</table>

[16] § 3 Nr. 18 TKG.
[17] § 3 Nr. 5 TKG.
[18] Vom 18. Dez. 2000; BGBl. I, 1740.
[19] § 2 Nr. 3 TDSV.
[20] Vom 22. Jan. 2002, auf Grund § 88 II 2, 3, IV 2, V 2 TKG.

2. Fernmeldegeheimnis[21], Art. 10 I, 3. Alt. GG

a) Schutzgut

Das Fernmeldegeheimnis in Artikel 8 Europäische Menschenrechtskonvention (EMRK) und Artikel 10 I GG dient der freien Entfaltung der Persönlichkeit durch Kommunikationsaustausch und schützt die Vertraulichkeit aller mit Mitteln des Fernmeldeverkehrs übermittelten Informationen, so z. B. den Fax-, Telefon- oder E-Mail-Verkehr[22].

aa) Schutzbereich

In den §§ 85 f. TKG wird das Telekommunikationsgeheimnis konkretisiert[23]. Ihm unterliegen sowohl der Inhalt als auch die „näheren Umstände" der Telekommunikation[24] (§ 85 I 1, 2 TKG).

Geschützt sind die Tatsache einer Telekommunikationsbeteiligung (das „Ob") und die Umstände (das „Wie" und „Wo") eines erfolglosen Verbindungsversuchs (§ 85 I 1 TKG). Der Übertragungsvorgang als solcher ist bereits geschützte Information[25].

bb) Eingriff und verfassungsrechtliche Rechtfertigung

Jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten durch den Staat ist als Grundrechtseingriff anzusehen[26].

Eingriffe in das Fernmeldegeheimnis bedürfen einer gesetzlichen Grundlage (Art. 10 II 1 GG). Das zum Eingriff berechtigende Gesetz muss dabei selbst verfassungsmäßig, d. h. verhältnismäßig sein sowie dem Bestimmtheits- und Zitiergebot genügen.

b) Unterscheidung §§ 100a, b und §§ 100g, h StPO

Die §§ 100a, b StPO rechtfertigen die Überwachung und Aufzeichnung der zukünftigen Telekommunikation unter strengen Voraussetzungen[27].

Bei einer Telekommunikationsüberwachung ist die Erhebung sowohl von Kommunikationsinhalten als auch von Verbindungsdaten möglich[28], wobei zurückliegende Verbindungsdaten nur nach § 100g und nicht nach § 100a StPO angefordert werden dürfen[29].

Die §§ 100g, h StPO sind hinsichtlich der Kommunikation enger gefasst. Sie umfassen nur TK-Verbindungsdaten, die § 100g III StPO abschließend aufzählt. Diese TK-Verbindungsdaten können sowohl in der Vergangenheit als auch – im Gegensatz zu § 12

---

[21] auf Grund technologischer Entwicklung auch: Telekommunikations-Geheimnis.
[22] BVerfGE 67, 152 (172); 100, 313 (358); BVerfG, Beschl. v. 9. Okt. 2002 – 1 BvR 1611/96; 805/98 – Abs.Nr. 19, www.bverfg.de; Jarass/Pieroth, Grundgesetz Kommentar, Art. 10, Rn 5.
[23] Beck`scher TKGK/Büchner § 85, Rn 1.
[24] St. Rspr.: BVerfGE 67, 157 (172) = NJW 1985, 121; BVerfGE 85, 386 (396); M/D/Herzog, Art. 10, Rn 15.
[25] von Münch/Kunig, Art. 10, Rn 22; BVerfGE 100, 313 (358).
[26] BVerfGE 85, 386 (398) (Fangschaltung); BVerfG, 1 BvR 2226/94, Abs.Nr. 186, www.bverfg.de.
[27] SK/StPO/Rudolphi, § 100a, Rn 45.
[28] Welp, S. 89; Schmidt, der Kriminalist 2002, 210 (211).

FAG – in der Zukunft liegen[30] (§ 100g I 3 StPO).

Übersicht: Telekommunikation, Normen

zurückliegende Kommunikation		Ab Anordnung	zukünftige Kommunikation	
TK-Inhalte, (-)		Telekom-munikation	TK-Inhalte, § 100a	
TK-Verbindungsdaten, § 100g	TK-Umstände	§ 85 I 1 TKG	TK-Umstände	TK-Verbindungsdaten, § 100g
Stand-By, (-)				Stand-By, § 100a § 100i

c) Inhaltsdaten und Verbindungsdaten

Fraglich ist, ob Verbindungsdaten ebenso schutzwürdig wie Inhaltsdaten sind.

Eine Auffassung sieht Verbindungsdaten nur als automatisch erzeugtes, technisches Nebenprodukt der Kommunikationsinhalte an. Verbindungsdaten verdienen danach nicht denselben Schutz[31] wie Kommunikationsinhalte.

Das Bundesverfassungsgericht aber hält Verbindungsdaten gegenüber Inhalten für nicht weniger schutzwürdig[32]. Durch Standort- und Anschlusskennung, Zeitpunkt, Dauer, Art der Kommunikation und Intensität der Kontakte lässt sich nämlich ein Profil des sozialen Umfeldes erstellen[33].“ Solche Verhaltensprofile „können die Aussagekraft von Inhaltsdaten erreichen oder im Einzelfall sogar übertreffen.“[34]

Dennoch ist die Auskunftserteilung im Gegensatz zur umfassenderen Telekommunikationsüberwachung ein weniger intensiver Eingriff[35].

d) Verpflichtete

Art. 10 I GG begründet neben einem Abwehrrecht auch die Pflicht des Staates, die Grundrechtsberechtigten vor Eingriffen Dritter zu bewahren, da es nach der Privatisierung und Öffnung des Telekommunikationsmarktes kein unmittelbar aus Art. 10 GG gebundenes Staatsunternehmen mehr gibt (Art. 87f GG[36]).

Diejenigen, die geschäftsmäßig TK-Dienste erbringen oder daran mitwirken (die Telekommunikationsunternehmen), sind dazu verpflichtet das Fernmeldegeheimnis zu wahren (§ 85 II 1 TKG). Eine Zuwiderhandlung führt zur Erfüllung des Tatbestandes des § 206 StGB[37].

Es ist diesen Verpflichteten durch Gesetz untersagt, über „das erforderliche Maß der

---

[29] Pfeiffer StPO, § 100a, Rn 1 a.E.
[30] Hilger, GA 2002, 228.
[31] z.B. KK/StPO/Nack, § 100a, Rn 18.
[32] BVerfGE 85, 386 (396).
[33] Welp, S. 90 f.; Weßlau, Datenschutz und neue Medien im Strafprozess, ZStW 2001, 681 (690).
[34] 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 07.08. Oktober 1999.
[35] Welp, S. 91.
[36] Gesetz zur Änderung des Grundgesetzes vom 30.08.1994; BGBl. I, S. 2245; BVerfG, 1 BvR 1611/96; 805/98, Abs.Nr. 21, www.bverfg.de.
[37] Welp, in Lenckner-FS, S. 619 ff.

geschäftsmäßigen Erbringung von TK-Diensten“ hinaus (§ 85 III 1 TKG), Kenntnis von der Telekommunikation zu erlangen. Regelmäßig sind zur Erbringung von Telekommunikationsleistungen nur Verbindungsdaten nötig[38].

Die Verwendung bzw. auch eine Weitergabe (zulässig) erlangter Kenntnisse über Verbindungsdaten, außer für Zwecke der Erbringung von TK-Leistungen, „ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf TK-Vorgänge bezieht“ (§ 85 III 2 TKG).

e) Ergebnis

Von der Unverletzlichkeit des Fernmeldegeheimnisses wird in Art. 10 II 1 GG dahingehend abgewichen, dass Beschränkungen - auf Grund eines Gesetzes - möglich sind.

3. Recht auf informationelle Selbstbestimmung - Art. 2 I/ Art. 1 I GG

Nach der Rechtsprechung des Bundesverfassungsgerichts[39] gewährt Art. 2 I i.V.m. Art. 1 I GG ein Recht des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, da es in der modernen Welt der elektronischen Datenverarbeitung kein „belangloses Datum“ mehr gibt. Das Recht auf informationelle Selbstbestimmung kann aber durch Gesetz eingeschränkt werden. Dieses muss verfassungsmäßig sein.

Das TKG und die TDSV regelt den Umgang mit personenbezogenen Daten im Bereich der Telekommunikation. Die Telekommunikationsunternehmen sind befugt, zur Entgeltermittlung und -abrechnung erforderliche Verbindungsdaten zu erheben und zu verarbeiten (§§ 85 III TKG, 7 II TDSV). Dabei sind nicht erforderliche Daten grundsätzlich unverzüglich zu löschen (§ 7 III 2 TDSV).

Gemäß § 7 III 3 TDSV können aber Verbindungsdaten von den TK-Unternehmen unter Kürzung der Zielrufnummer um die letzten drei Ziffern höchstens sechs Monate nach Versendung der Rechnung zu Beweiszwecken gespeichert werden.

Ein Auskunftsanspruch ist jedoch nutzlos bei gekürzten Zielrufnummern, sodass bei der Anforderung zukünftiger VD die TK-Anbieter aufgefordert werden können, vorhandene Daten nicht zu löschen, sondern bis zum „Abruf“ zu speichern.

Dadurch wird in das Recht auf informationelle Selbstbestimmung eingegriffen.

Nach Auffassung des BVerfG[40] wird jedoch bei Vorliegen eines Eingriffs in das Telekommunikationsgeheimnis (Art. 10 I, 3. Alt. GG) das allgemeine Persönlichkeitsrecht als da allgemeinere Recht verdrängt.

---

[38] Beck`scher TKGK/Büchner § 85, Rn 6; ausführlich: Welp, S. 15 (17).
[39] BVerfGE 65, 1 (42 f.) „Volkszählung“.
[40] BVerfGE 67, 157 (171); BVerfG 1 BvR 2226/94 = E 100, 313 ff., Abs.Nr. 158; www.bverfg.de.

4. Wirksame Strafverfolgung

a) Anspruch der Allgemeinheit auf wirksame Strafverfolgung

Aus dem Rechtsstaatsprinzip leitet das Bundesverfassungsgericht ab, dass es Ziel einer funktionsfähigen Strafrechtspflege sei, „Gerechtigkeit" zu verwirklichen[41]. Das strafprozessuale Beweisrecht ist auf die Ermittlung der materiellen Wahrheit angelegt[42].

Ein besonderes Interesse der Allgemeinheit besteht an der Aufklärung schwerer Straftaten[43]. Dabei ist dieses Interesse im Verhältnis zu den Grundrechten des Beschuldigten zu setzen, d.h. eine Abwägung vorzunehmen.

b) Echter strafprozessualer Grundrechtseingriff

So genannte „echte" strafprozessuale - den Strafprozess fördernde - Grundrechtseingriffe[44] wie die Überwachung des Fernmeldeverkehrs (§ 100a StPO) dienen der Sicherung von Beweismitteln[45].

Die Anordnung von TK-Verbindungsdaten dient ebenfalls der Sicherung von beweiserheblichen Tatsachen, z.B. dass ein Täter im Vorfeld eines Deliktes mit Komplizen Verbindung aufgenommen oder sich während der Tatzeit in der Umgebung des Tatortes aufgehalten hat.

5. Repression, Prävention

Die Anforderung von Verbindungsdaten ist als strafprozessualer Grundrechtseingriff auf die Strafverfolgung gerichtet. Eingriffsgrundlage ist § 100g StPO.

In den Polizeigesetzen der Länder sind vergleichbare Regelungen zur Gefahrenabwehr (noch)[46] nicht enthalten. Lediglich in Niedersachsen (1994) und in Hessen (2001) gibt es die Möglichkeit zur Verwendung von Verbindungsdaten[47], z.B. zum Auffinden eines Suizidgefährdeten mittels Standortkennung.

B. Anwendungsbereich der §§ 100g, h StPO

[41] BVerfGE 33, 367, 383; Gusy, StV 2002, 153 (154).
[42] BVerfGE 77, 65 (76); Welp, NStZ 1994, 215.
[43] BVerfGE 29, 183 (194); 33, 367, 383.
[44] Amelung, JZ 1987, 737 (739).
[45] Amelung, JZ 1987, 737 (739) m.w.N.
[46] Aktuell planen mehrere Bundesländer eigene Gesetze zur Überwachung von Telekommunikationsvorgängen; „Jedem Bundesland sein Lauschgesetz": www.heise.de, 23.11.2002.
[47] Schmidt, der Kriminalist 2002, 210 (211).

I. Auskunftspflicht

1. Keine Auskunftspflicht von Diensteanbietern i.S.d. § 3 Nr. 1 TDG[48]

Zu beachten ist, dass durch § 100g StPO nur die Auskunft zu Verbindungsdaten der Telekommunikation angefordert werden können, die die Telekommunikationsunternehmen erbringen. Die §§ 100g, h StPO sind keine Eingriffsgrundlagen für Daten von Tele-Diensteanbietern i.S.d. § 3 TDG.

Teledienste sind „alle Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten [...] bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt“ (§ 2 I TDG), z.B. Telebanking oder Informationsangebote (§ 2 II Nr. 1, 2 TDG).

2. Gegenstand

In § 100g III StPO werden diejenigen TK-Verbindungsdaten abschließend aufgezählt, deren Auskunftserteilung angeordnet werden darf.

„Telekommunikationsverbindungsdaten sind:

1. im Falle einer Verbindung
   Berechtigungskennungen,
   Kartennummern,
   Standortkennung sowie
   Rufnummern oder *Kennung* des anrufenden und angerufenen Anschlusses oder der *Endeinrichtung*,
2. Beginn und Ende der Verbindung nach Datum und Uhrzeit,
3. vom Kunden in Anspruch genommene Telekommunikationsdienstleistung
4. Endpunkte festgeschalteter Verbindungen, ihr Beginn und ihr Ende nach Datum und Uhrzeit.“

Von den aufgezählten Verbindungsdaten darf der TK-Kommunikationsdiensteanbieter Kenntnis nehmen, soweit sie zur geschäftsmäßigen Erbringung der Dienstleitungen erforderlich sind (§ 85 II 1 TKG).

Gemäß § 6 I i.V.m. § 7 TDSV dürfen Verbindungsdaten u.a. zur Entgeltberechnung erhoben, verarbeitet und genutzt werden. Der Katalog des § 100g III StPO richtet sich nach der in § 6 I TDSV genannten Aufzählung.

a) Standortkennung, Funkzelle (§ 100g III Nr. 1 StPO)

Unter der Standortkennung sind die gespeicherten Funkzellen- bzw. Rufzonen-Daten gemeint.

Die Funkzelle wird als „der Versorgungsbereich innerhalb eines Versorgungsnetzes“ definiert, „der eine bestimmte geographische Fläche abdeckt.“[49]

---

[48] Gesetz über die Nutzung von Telediensten vom. 22. Juli 1997 (BGBl. I, S. 1870), zuletzt geändert durch Artikel 1 EGG vom 14. 12.2001 (BGBl. I, S. 3721).

[49] § 4 Nr. 5 TKÜV; Rufzone: § 4 Nr. 9 TKÜV.

aa) „Im Falle einer Verbindung“

Beim Aufbau einer TK-Verbindung wählt sich das Mobiltelefon in eine Funkzelle ein. Auf Grund dieser Daten – Erhebung und Speicherung zur Entgeltberechnung erforderlich und daher zulässig - ist die Bestimmung des Aufenthaltsortes des TK-Teilnehmers auf die Funkzelle genau zum Zeitpunkt der Verbindung möglich[50]. Damit kann ein noch unbekannter Täter identifiziert werden, wenn während eines bestimmten Zeitraumes in einer bestimmten Funkzelle eine TK-Verbindung bestand[51].

Aus diesen Standortdaten lässt sich bei längeren TK-Verbindungen und Durchquerung mehrerer Funkzellen ein sog. rudimentäres Bewegungsprofil erstellen[52].

bb) Exkurs: Stand-By-Daten, § 100i StPO

Aber auch ein Mobilfunkgerät im Stand-By-Betrieb sendet regelmäßig Lokalisierungsinformationen aus. Diese Daten sind gesprächsunabhängig, sie werden nicht gemäß § 6 I TDSV gespeichert und lediglich zur Verbindungsherstellung und zur Sende-Steuerung benötigt[53]. Wie bereits § 12 FAG enthält auch § 100g StPO keine Auskunftspflicht über Stand-By-Daten.

Im Gegensatz zu § 100a StPO: Obwohl in der Literatur und Lehre[54] weitgehend abgelehnt, hat u.a. der BGH eine Auskunftspflicht bezüglich des Standorts von nicht telefonierenden Mobilfunkgeräten angenommen[55], da dieses vom TK-Vorgang „unabhängige“ Datum zumindest kommunikationserheblich ist und darum § 100a StPO unterfalle. Diese verfassungsrechtlich bedenkliche Ansicht spielt im zu erörterten Fall keine Rolle. Stand-By-Daten sind im Rahmen des § 100g StPO nicht auskunftspflichtig[56]. Sie werden nicht gespeichert, da sie für Kommunikation und Entgeltabrechnung nicht erforderlich sind (vgl. § 85 III 1 TKG).

Mit Einführung des neuen § 100i StPO[57] wird nun ausdrücklich die Standortbestimmung von Mobilfunkgeräten in Stand-By unter bestimmten Voraussetzungen durch technische Mittel (IMSI-Catcher) zugelassen (§ 100i I Nr. 2, II 2 StPO).

b) Kartennummer, Kennung des Anschlusses

Bei der Herstellung einer TK-Verbindung senden Mobilfunkgeräte eine Kartenkennung - die sog. IMSI, das technische Äquivalent zur Rufnummer - und eine Gerätekennung (IMEI) aus[58]. Die Auskunftspflicht erstreckt sich sowohl auf den angerufenen als auch auf den anrufenden Anschluss bzw. die Endeinrichtung. Unter einer Endeinrichtung ist eine Einrichtung zu verstehen, die an ein Telekommunikationsnetz angeschlossen

---

[50] Welp, S. 29.
[51] BT-Drs. 14/7258, S. 4.
[52] Schmidt V., der Kriminalist 2002, 210
[53] Welp, S. 30.
[54] Malek/Wohlers, Zwangsmaßnahmen und Grundrechtseingriffe, Rn 425; BGH, NStZ 2002, 103 f.; Kudlich, JuS 2002, 1165 (1169): „§ 100a StPO [...] `Supereingriffsbefugnis`“.
[55] LG Dortmund, NStZ 1998, 577; LG Aachen, StV 1999, 590; Ravensburg, NStZ-RR 1999, 84; KK/StPO/Nack, § 100a, Rn 13; BGH, NJW 2001, 1578.
[56] BR-Drs 702/01, S. 8; BGH, StV 2001, 214; § 2 Nr. 4 TDSV.
[57] Gesetz zur Änderung der Strafprozessordnung vom 06.08.2002, BGBl. I, S.3018; Hilger, Gesetzgebungsbericht, GA 2002, 557 ff.
[58] IMSI = International Mobile Subscription Identity; IMEI= International Mobile Equipment Identity.

werden soll (vgl. § 3 Nr. 3 TKG), z.B. Computer, Telefon.

Umstritten war, ob die Gerätekennung ein geeignetes Merkmal zur Individualisierung einer zukünftig zu überwachenden Telekommunikation sei[59]. Da aber im Bereich organisierter Kriminalität (OK) tätige Personen mehrere Anschlussnummern und „Handys" zur Verfügung haben, ist eine Kontrolle der Verbindungsdaten nur noch sinnvoll, wenn auch Mobiltelefone und nicht nur die Anschlüsse (SIM-Karten), die sich bei wechselnden Mobilfunkkarten ändern, in eine Anordnung einbezogen werden[60].

Von den in § 100g III Nr. 1 StPO genannten Kennungen ist nun auch ausdrücklich die Gerätekennung mitumfasst.

Bloße Stamm- bzw. Vertragsdaten unterfallen dagegen nicht der Pflicht zur Auskunft gem. § 100g StPO. Die Betreiber sind bereits nach § 89 VI 1 TKG dazu verpflichtet[61].

Wie bei der Standortkennung, besteht eine Auskunftspflicht bezüglich der Kartennummer und Anschlusskennung gem. § 100g StPO nur, „im Falle einer Verbindung".

Jedoch besteht die Möglichkeit, dass diese Kennungen gem. § 100i StPO mit Hilfe eines IMSI-Catchers von aktiv geschalteten Mobiltelefonen ermittelt werden können, auch wenn keine Verbindung zu Stande gekommen ist.

c) Endpunkt, Beginn und Ende der Verbindung, Art der Telekommunikation (§ 100g III Nr. 2-4)

Die in Absatz 3 Nr. 2-4 genannten Verbindungsdaten Zeitpunkt, Beginn und Ende, Dauer sowie die Art der Telekommunikation können angefordert werden.

Sie sind zur Erbringung von Telekommunikationsdienstleistungen, insbesondere zur Entgeltberechnung, nötig (vgl. § 85 III TKG).

3. Informationsbeschaffung

§ 100g StPO berechtigt und verpflichtet diejenigen, die geschäftsmäßig Telekommunikations-Dienstleistungen erbringen oder daran mitwirken zur unverzüglichen Erteilung von Auskünften. Dabei sind die TK-Betreiber nicht berechtigt, selbst Maßnahmen zu treffen und Informationen zu beschaffen. Die Auskunftspflicht bezieht sich lediglich auf das rechtmäßig erworbene Wissen der TK-Unternehmen. Ihnen ist es gemäß §§ 85 III 1 TKG, 100g StPO nicht erlaubt auf Inhaltsdaten zuzugreifen, so auch nicht auf gespeicherte Nachrichten in einer Mail-Box[62].

---

[59] Krit.: Beck`scher TKGK/Ehmer § 88, Rn 3; Deckers, StV 2002, 109 (112).

[60] Ramelsberger, SZ 25.10.2001, S. 2; Deckers, StV 2002, 109 (110); **zu § 12 FAG**: IMEI keine Kennung, LG Hamburg MMR 1998, 419; aA. BGH-Ermittlungsrichter, MMR 1999, 99.

[61] Variable IP-Adressen sind keine Bestandsdaten; AG Ulm, Beschluss v. 8.4.2002 -3 Gs 413/02; LG Ulm, B. v. 21.3.2002 -2 Qs 2016/02; zu allgemein: BR-Drs. 702/01, S. 9.

[62] KK/StPO/Nack § 100a, Rn 7 ff; Welp, NStZ 1994, 209 (212); M/D/Herzog/Scholz, Art 10, Rn 56 (58);

Die Pflicht zur Auskunftserteilung bezieht sich nur auf elektronisch gespeicherte Informationen, die nur maschinell gelesen werden können.

§ 85 TKG beinhaltet die Befugnis, von Verbindungsdaten Kenntnis zu nehmen, die für die Entgeltberechnung notwendig sind[63]:

1) Regelmäßig ist nur der abgehende Telekommunikationsverkehr entgeltpflichtig (nur der Anrufer, nicht der Angerufene, zahlt für die Verbindung)
2) Die Kenntnisnahme von Verbindungsdaten eingehender Verbindungen ist für die Entgeltberechnung beim angerufenen TK-Teilnehmer nicht erforderlich.

   Der TK-Betreiber darf daher von diesen Daten keine Kenntnis nehmen (§ 85 III 1 TKG).

Da aber der Anrufende selbst die Kosten zu tragen hat, ist bei der Erstellung seiner Rechnung die Kenntnisnahme seiner Verbindungsdaten geschäftlich notwendig. Somit lassen sich die an den Beschuldigten „gerichteten" TK-Daten in die Auskunftspflicht einbeziehen.

A ⟶ B

Anrufer, TK-VD von A — Angerufener; keine VD von ihm, aber seine Rufnummer ist Bestandteil der Verbindungsdaten des A

4. Adressat der Auskunftspflicht

Ursprünglich war die nach § 12 FAG Verpflichtete die Deutsche Bundespost als alleinige Betreiberin von Fernmeldeanlagen. Einen ausdrücklichen Adressaten enthielt die Vorschrift daher nicht.

§ 100g StPO nennt als Adressaten der Auskunftspflicht diejenigen, die geschäftsmäßig TK-Dienstleistungen erbringen[64], d.h. die Deutsche Telekom und alle anderen privaten Anbieter von Telekommunikationsdienstleistungen. § 88 TKG regelt i.V.m. der TKÜV die technische Umsetzung von Überwachungsmaßnahmen, und legt den Verpflichteten die Kosten der Überwachung auf[65].

II. Materielle Eingriffsvoraussetzungen

Der frühere § 12 I 1 FAG machte (im Gegensatz zu § 100a StPO) die Eingriffsbefugnis von keinerlei materiellen Voraussetzungen abhängig. Bezüglich des Umfangs der Beschränkungen war § 12 FAG unbestimmt. Mangels Eingriffsgrenzen (mangelnde Verhältnismäßigkeit) war er verfassungsrechtlich als sehr bedenklich anzusehen bzw. verfassungswidrig[66].

§ 100g StPO ist enger gefasst als § 12 FAG, die Eingriffsschwelle für Auskunftsverlan-

---

SK/StPO/Rudolphi § 99, Rn 19.

[63] Beck`scher TKGK/Büchner § 85, Rn 6.

[64] Vgl. § 100b III 1 StPO; § 3 Nr. 5 TKG.

[65] Zur Verfassungsmäßigkeit der Kostentragungspflicht: Koenig/Koch/Braun, KuR 2002, 289 (294).

[66] Welp, S. 83, 98; von Mangoldt/Kleinknecht/Schmidt/Gusy, Art. 10, Rn 69, 71.

gen wurde angehoben[67].

Der § 100g StPO reiht sich in die seit 1968[68] eingeführte Regelungstechnik ein. Strafprozessuale Eingriffe sind an bestimmte Delikte gebunden, für die ein gewisser Tatverdacht sprechen muss. Ein Eingriff ist danach unzulässig, wenn er nicht erforderlich ist, d.h. wenn es mildere gleich wirksame Mittel gibt[69].

1. Anlasstaten

Da ein Grundrechtseingriff verhältnismäßig sein muss, darf dessen Intensität nicht „außer Verhältnis zur Bedeutung der Sache und dem vom Bürger hinzunehmenden Einbußen stehen“[70].

Eine Auskunftspflicht bezüglich TK-Verbindungsdaten besteht daher nur, wenn die Eingriffsbefugnis auf bestimmte Deliktskategorien begrenzt wird, wenn z.B. ein objektivierbarer Verdacht bezüglich einer „Straftat von erheblicher Bedeutung“ oder bzgl. einer Straftat mittels einer Endeinrichtung vorliegt (§ 100g I 1 StPO).

Die Eingriffsschwere soll in angemessener Relation zur Wahrnehmung von Strafverfolgungsinteressen stehen[71].

a) Katalogtat (§ 100a StPO)

Zunächst verweist § 100g StPO auf den Katalog der Deliktstypen, auf Grund deren Verdacht eine umfangreiche Telefonüberwachung möglich ist. Nach dem Wortlaut ist diese Verweisung jedoch nur beispielhaft.

Der Wortlaut wird sinnvollerweise dahingehend verstanden, dass bei Katalogtaten, die erhebliche Bedeutung zu unterstellen ist. Soweit eine Katalogtat vorliegt, die nicht von erheblicher Bedeutung ist, ist dennoch eine Anlasstat anzunehmen und eine Anordnung gemäß § 100g StPO möglich[72].

b) Straftat von erheblicher Bedeutung (Generalklausel)

Eine „Straftat von erheblicher Bedeutung“ ist relativ unbestimmt. § 100a StPO soll zu dessen Ausgestaltung eine „materielle Leitbildfunktion“ erfüllen[73].

Danach muss das erhebliche Delikt mindestens eines der mittleren Kriminalität sein[74], hinsichtlich des geschützten Rechtsguts, der tatbestandsmäßigen Handlung und des Strafrahmens mit einer Katalogtat des § 100a StPO wenigstens annähernd vergleichbar

---

[67] Wollweber, NJW 2002, 1554.
[68] Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10), BGBl. I 1968, S. 949; BGBl. I 1992, S. 1302 (Schleppnetzfahndung); BGBl. I 1998, S. 846 (Lauschangriff).
[69] Welp, S. 37.
[70] St. Rspr. BVerfG, NJW 2000, 55, 56; AK/GG/Bizer, Art. 10, Rn 78.
[71] Welp, S. 20.
[72] Näheres: Welp, GA 2002, 235 (236).
[73] Wollweber, NJW 2002, 1554.

sein[75]. Damit lassen sich auch Taten aus den Katalogen der §§ 81g, 110a StPO (Sexualdelikte, besonders schwerer Diebstahl; Betäubungsmittel-, Waffen-, Bandendelikte) unter § 100g StPO subsumieren[76].

c) Straftat mittels Endeinrichtung

aa) Wortlaut, Systematik, Wille des Gesetzgebers

Wenn eine Straftat mittels einer Endeinrichtung (§ 3 Nr. 3 TKG, z.B. Telefon, Internet-Computer) begangen wurde, braucht keine erhebliche Straftat gegeben zu sein (so der Wortlaut des § 100g I 1 2. Alt. StPO).

- Entgegen dem Wortlaut des § 100g StPO hat nun das LG Köln[77] entschieden.

Durch systematische Auslegung im Zusammenhang mit § 100h I 2 StPO gelangt es zu dem Ergebnis, dass auch bei einer Straftat mittels einer Endeinrichtung eine erhebliche Straftat vorliegen müsse, wenn Name und Anschrift, Rufnummer oder eine andere Kennung des Betroffenen unbekannt sind. Der Wortlaut des § 100h I 2 StPO erlaube eine Auskunftsanordnung bei namentlich unbekannten Tätern nur bei Vorliegen einer Straftat erheblicher Bedeutung und nicht im Bereich der Bagatellkriminalität[78].

- Nach dem Willen des Gesetzgebers ist dieses Ergebnis aber gerade nicht gewollt. Bei Straftaten mittels Endeinrichtung werde keine erhebliche Straftat verlangt. Auch bei weniger schweren Delikten soll eine Auskunft möglich sein, da ohne Rückgriff auf die TK-Verbindungsdaten Ermittlungen bei Beleidigungen oder sexuellen Belästigungen über Telefon, SMS oder E-Mail beinahe aussichtslos seien[79].

- Die Straftat mittels Endeinrichtung ist neben der erheblichen Straftat eine gleichgeordnete Alternative (§ 100g I 1 StPO). Eine Auskunft darf aber bei unbekannten Namen oder Kennungen ausdrücklich nur bei Vorliegen einer erheblichen Straftat angeordnet werden (§ 100 h I 2 StPO). Durch § 100h wird die Weite des Regelungsbereiches des 100g StPO hinsichtlich einer Straftat mittels Endeinrichtung eingeengt bzw. konkretisiert, soweit Name und/oder Kennung eines Verdächtigen nicht bekannt sind. Entgegen dem Willen des Gesetzgebers muss in einem solchen Falle eine Straftat von erheblicher Bedeutung vorliegen. Diese Lösung ist auch hinsichtlich der verfassungsrechtlichen Verhältnismäßigkeit der Maßnahme vorzuziehen

---

[74] BVerfGE 103, 21 (34) = NJW 2001, 879; .

[75] Wollweber, NJW 2002, 1554; kritisch zur Bestimmtheit: Welp, GA 2002, 535 (540).

[76] Vgl. Schmidt, der Kriminalist 2002, 210 (212).

[77] Beschl. v. 05.02.2002 – 107 Qs 36/02: keine Auskunftspflicht bei Bagatellkriminalität; vgl. AG Wuppertal, Beschl. v. 21.01.02 -8 (B) Gs 25/02; AG Ulm, Beschl. v. 14.02.2002 – 4 Gs 234/02; RA Frank Feser, www.bonnanwalt.de,.

[78] Welp, GA 2002, 535 (541); SK/Wolter, § 100g, Rn 16: Bei wiederholenden Telefonattacken ist eine „Fangschaltung“ das mildere Mittel (§ 10 TDSV).

bb) „mittels“

Die tatbestandsmäßige Handlung muss mittels einer Endeinrichtung begangen wurden sein. Wiederholtes Anrufen, um An- und Abwesenheit für einen späteren Diebstahl herauszufinden, zählt nicht dazu. Dagegen greift § 100g I 1 StPO, wenn der Mittäter das Opfer telefonisch ablenkt, damit ein Diebstahl begangen werden kann.

Die Telekommunikation muss final eingesetztes Mittel für eine Straftat sein.

d) Begehung, Versuch, Vorbereitung

§ 100g I StPO findet nur Anwendung, wenn eine in Satz 1 genannte Tat begangen, strafbar versucht oder vorbereitet wurde.

e) Zusammenfassung

Eine Auskunftspflicht beschränkt sich auf bestimmte Anlasstaten und besteht nicht bei minderschweren Delikten und Ordnungswidrigkeiten (§ 46 I, III 1 OWiG). Dies ergibt sich bereits aus dem Verhältnismäßigkeitsgrundsatz[80].

2. Verdacht

a) Deliktsverdacht, Bestimmte „Tatsachen“

Der § 12 I 1 FAG stellte keine Anforderungen an den Verdachtsgrad[81]. Es genügten daher „zureichend tatsächliche Anhaltspunkte“ (§ 152 II StPO) bzgl. irgendeiner Straftat.

§ 100g I 1 StPO verlangt, dass „bestimmte Tatsachen“ den Verdacht der Begehung einer in Satz 1 genannten Taten begründen. Dieser Verdacht braucht - wie bei § 100a StPO - weder hinreichend noch dringend (§§ 203, 112 I 1 StPO) zu sein[82].

Als Verdachtsgrundlage kommen glaubhafte Zeugenaussagen aber auch logische Schlussfolgerungen, nicht jedoch reine Vermutungen in Betracht[83].

b) Personenverdacht

§ 100g I 1 StPO ist nur einschlägig, wenn die Anordnung die in Satz 2 genannten Personen betreffen. Dazu zählen der beschuldigte Täter/ Teilnehmer und diejenigen, von denen anzunehmen ist, „dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben“ oder der Beschuldigte ihren Anschluss benutzt[84].

3. Erforderlichkeit

---

[79] BT-Drs. 14/7008, S. 6, 7.
[80] Hilger, GA 2002, 228 (229); BR-Drs. 702/01, S. 7; SK/Wolter, § 100g, Rn 12.
[81] SK/StPO-Rudolphi, § 100a, Rn 11.
[82] Bär, MMR 2002, 358 (360); SK/StPO/Rudolphi, § 100a, Rn 11; Bernsmann/Jansen, StV 1998, 217 (219).
[83] Schmidt, der Kriminalist 2002, 210 (213); Bär, MMR 2002, 358 (360).
[84] § 100g I 2 i.V.m. § 100a S. 1 StPO.

Auf Grund § 12 FAG konnten Verbindungsdaten - gemäß Wortlaut - ohne Rücksicht auf ein milderes Mittel angefordert werden[85].

Die Möglichkeit einer Auskunftsanforderung besteht nunmehr nur noch, wenn sie zur Untersuchung erforderlich ist (§ 100g I 1 StPO). Der Begriff der Erforderlichkeit weist darauf hin, dass eine Auskunft nur angefordert werden darf, wenn der Grundsatz der Verhältnismäßigkeit beachtet wurde[86].

Eine Anordnung ist verhältnismäßig, wenn der vom Staat verfolgte Zweck zulässig ist, das eingesetzte Mittel dem Zweck dient, geeignet, notwendig und angemessen ist[87].

Die Auskunftsanordnung als strafprozessualer Grundrechts-Eingriff dient u.a. der Wahrheitsfindung und Beweissicherung[88] im Ermittlungsverfahren. Eine Anordnung ist durchaus geeignet die Wahrheit herauszufinden und Beweise zu sichern. Vom Einzelfall ist abhängig, ob die weiteren Grundsätze der Verhältnismäßigkeit eingehalten werden.

4. Subsidiarität – Zielwahlsuche (§ 100g II StPO)

§ 100g II StPO legt fest, dass eine Zielwahlsuche[89] nur angeordnet werden darf, wenn „die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre."

Die erhöhte Eingriffsschwelle ist dadurch bedingt, dass meist eine hohe Zahl von Verbindungsdaten unverdächtiger Personen in eine Recherche (vergleichbar der Rasterfahndung) einbezogen werden. Eine Zielwahlsuche bezieht sich auf den Gesamtbestand gespeicherter Daten eines TK-Unternehmens.

Durch eine Zielwahlsuche werden unbekannte Anschlussnummern ermittelt, von denen TK-Verbindungen zu einem bekannten Anschluss hergestellt worden sind. Dazu werden alle gespeicherten Verbindungsdaten mit der fraglichen Nummer abgeglichen. Die bei einem Abgleich erzielten „Treffer" werden in einer Datei gespeichert. Es lässt sich dann sowohl eine positive als auch die negative Aussage über das Zustandekommen von TK-Verbindungen treffen.

Da bereits die Speicherung von Verbindungsdaten[90] ein Grundrechtseingriff ist, ist der durch Suchroutinen gezielte Zugriff auf einzelne Datensätze und der Datenabgleich

---

[85] Welp, S. 41.
[86] Wollweber, NJW 2002, 1554 (1555); Pfeiffer StPO § 100a, Rn 5.
[87] Pieroth/Schlink, Grundrechte, Rn 279 ff.
[88] Amelung, JZ 1987, 736 (739); Gusy, StV 2002, 153 (155).
[89] = Recherche und Auskunft, ob von einem TK-Anschluss eines Dritten eine Verbindung zum Beschuldigten/ Nachrichtenmittler hergestellt wurde (Hilger GA 2002, 228 [229]; Bizer, DuD 2002, 237; Weßlau, ZStW 2001, 692 ff.
[90] BVerfGE 65, 1 (43); 85, 386, 387.

ebenfalls ein Eingriff[91]. Dabei spielt es keine Rolle, ob Informationen dieses Abgleichs wieder spurenlos vernichtet werden. Spurenlosigkeit eines maschinellen Abgleichs ist Merkmal jeder elektronischen Rasterung[92].

Mit einer Subsidiaritätsklausel reiht sich der § 100g StPO in die „moderne“ übliche Regelungstechnik strafprozessualer Grundrechtseingriffe ein: Würde das jeweilige Mittel nicht eingesetzt, wäre eine Aufklärung aussichtslos oder wesentlich erschwert[93], oder aber andere Ermittlungen wären „erheblich weniger erfolgsversprechend oder wesentlich erschwert“[94].

Diese strafprozessualen Grundrechtseingriffe sind subsidiär gegenüber anderen Ermittlungsmethoden, die zur Erreichung desselben Aufklärungsziels geeignet sind.

III. Persönlicher Anwendungsbereich, Betroffene des Auskunftsanspruchs

§ 100g I 2 StPO erlaubt die Auskunftsanordnung über Verbindungsdaten des Beschuldigten und der Personen, von denen auf Grund „bestimmter Tatsachen“ anzunehmen ist, dass sie als Nachrichtenmittler des Beschuldigten fungieren oder der Beschuldigte ihren Anschluss benutzt (vgl. § 100g I 2 i.V.m. § 100a S. 2 StPO).

1. Beteiligung des Beschuldigten

Die Zulässigkeit eines Eingriffs ist von der Beteiligung des Beschuldigten am Telekommunikationsverkehr abhängig. Die Beschuldigteneigenschaft setzt voraus, dass der Verdacht einer Straftat besteht (s.o.) und ein Ermittlungsverfahren eingeleitet ist[95].

Es muss ein Verdacht bzgl. einer Person bestehen, die jedoch noch nicht identifiziert zu sein braucht[96]. Die Identität dieser Person ist zumeist erst das Ergebnis der Ermittlungen[97]. Es sind daher auch Ermittlungen gegen unbekannt möglich, wenn zumindest die Möglichkeit einer Individualisierung besteht.

Die Begrenzung des Eingriffs auf den Beschuldigten dient dem Schutz des TK-Verkehrs derjenigen Personen, die weder der Tat verdächtig sind, noch an einem TK-Vorgang beteiligt waren. Es ist eine sog. „Opfergrenze“ einzuhalten; auf Grund des Verhältnismäßigkeitsprinzips ist diese gegenüber Unbeteiligten eng zu bemessen[98].

---

[91] BVerfGE 65, 1 (43f.); 85, 386 (398); Welp, S. 100.
[92] Welp, S. 105
[93] Vgl. §§ 100c I Nr. 2, II S. 3; 100a I 3 StPO (kleiner Lauschangriff, technische Observationsmittel, Einsatz verdeckter Ermittler)
[94] Vgl. §§ 98a I 2, 163e I 2 StPO (Rasterfahndung, Ausschreibung zur polizeilichen Beobachtung); näheres Welp, S. 41, 42.
[95] Pfeiffer StPO § 52, Rn 5.
[96] SK/StPO/Rudolphi, § 100a, Rn 12.
[97] Vgl. LG Stuttgart, NJW 2001, 455 ff.
[98] Stein, in: Grünwald-FS, S. 865; vgl. Verhinderung allgemeiner Überwachungsmaßnahmen: AK/StPO/Amelung, § 99, Rn 5; SK/Rudolphi, § 99, Rn 10.

2. Individualisierungsfaktoren, Unverdächtige

Da üblicherweise Verbindungen, auf die sich der Eingriff bezieht, nur durch Anschlusskennungen individualisiert werden können, ist es nicht unwahrscheinlich, dass Dritte den Anschluss des Beschuldigten und der Beschuldigte Anschlüsse von Dritten benutzt. Ein Auskunftsersuchen kann sich auch (unter Voraussetzung) gegen Unverdächtige richten[99].

a) Nachrichtenmittler

Dabei muss aber „auf Grund bestimmter Tatsachen anzunehmen" sein, dass der Dritte „für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen" entgegennimmt oder weitergibt. Wird eine unverdächtige Person (auch gutgläubig) als Nachrichtenmittler tätig, so sind auch diese Verbindungsdaten auskunftspflichtig.

b) Anschlussüberlasser

§ 100g StPO ist aber auch anwendbar, wenn der Anschluss eines Dritten (z.B. Gastwirt, Freunde) vom Beschuldigten genutzt wird (s. § 100a S. 2 StPO). Kenntnis von dieser „Überlassung" muss ein solcher Dritter nicht haben[100].

c) Durch „Funkzellenabfrage" betroffene, unbeteiligte Personen

Im Gegensatz zu § 12 FAG wird die Auskunft über Verbindungsdaten auch auf lediglich räumlich und zeitlich bestimmte Kommunikation ausgedehnt. Telefoniert ein unbekannter Täter während der Tat oder in der Umgebung des Tatortes mit einem Mobiltelefon, sind dessen Verbindungsdaten zunächst in der nächsten Mobilfunkturm gespeichert. Bei hinreichend räumlich und zeitlicher Bestimmtheit der Telekommunikation ist nun unter den Voraussetzungen einer Subsidiaritätsklausel (§ 100h I 2 StPO) eine Auskunftsanordnung hinsichtlich aller in der Funkzelle zum Tatzeitpunkt getätigten Kommunikation möglich[101]. Dabei werden zwangsläufig auch Verbindungsdaten von völlig Unbeteiligten verarbeitet. Da in deren Grundrechte eingegriffen wird, ist diese Form der Auskunftsanordnung nur möglich, wenn anderenfalls die Erforschung des Sachverhalts aussichtslos oder wesentlich erschwert wäre (§ 100h I 2 StPO).

3. Beweisbedeutung

Eine Auskunft muss für die Untersuchung Bedeutung haben. Hat sie für das Ermittlungsverfahren voraussichtlich keine Bedeutung, darf sie nicht erhoben werden, da ein strafprozessualer Eingriff nur durch den Verfahrenszweck legitimiert ist[102].

---

[99] Verweis auf § 100a S. 2; BVerfGE 30, 22; BGHSt 29, 25 = NJW 1980, 67.
[100] SK/StPO/Rudolphi, § 100a, Rn 15; Bär, MMR 2002, 359 (362); z.B. Hacker-Angriffe.
[101] Bizer, DuD 2002, 237; BT-Drs. 14/7258, S. 4.
[102] Amelung, JZ 1987, 734 (739); Welp, S. 51.

IV. Zeitlicher Anwendungsbereich

Der § 12 I 1 FAG bezog sich gemäß seinem Wortlaut (durchgehende Verwendung des Imperfekts) nur auf Verbindungsdaten, die in der Vergangenheit lagen. Ein Auskunftsersuchen hinsichtlich zukünftiger Verbindungsdaten war nach hM unzulässig[103].

Der TK-Verkehr musste in der Vergangenheit abgeschlossen sein. Lediglich in der Rechtsprechung vereinzelter Gerichte[104] wurde auch eine Auskunftspflicht bezüglich zukünftiger Verbindungsdaten bejaht, da die zeitlichen Grenzen durch wiederholende Anordnungen umgangen werden konnten. Der Wortlaut als äußerste Grenze der Auslegung lässt ein solches Ergebnis jedoch nicht zu.

§ 12 I 1 FAG diente der „Kontrolle“ von Datenspuren nach einer beendeten TK. Ein Eingriff in zukünftige Verbindungsdaten konnte nur auf § 100a StPO gestützt werden und nur unter dessen Voraussetzungen[105].

Durch § 100g II StPO lässt der Gesetzgeber nun ausdrücklich auch eine Auskunftspflicht bzgl. zukünftiger Verbindungsdaten zu. Die TK-Unternehmen speichern daraufhin die Daten ohne Kürzung bis zur Auskunftserteilung (§ 3 I TDSV)[106].

Mit Verweis auf § 100b II 4, IV StPO wird klargestellt, dass diese Verbindungsdaten auf höchstens drei Monate herausverlangt werden können. Eine Verlängerung um weitere drei Monate ist möglich, wenn die Voraussetzungen der §§ 100g, h StPO weiterhin vorliegen.

Wenn die Voraussetzungen einer Auskunftserteilung nicht mehr vorliegen, ist die „Maßnahme“ einzustellen und der Richter sowie das TK-Unternehmen zu benachrichtigen (§ 100h I 3 a.E. i.V.m. § 100b IV StPO).

V. Formeller Anwendungsbereich (§ 100h StPO)

1. Bestimmtheit (§ 100h I 1, 2 StPO)

Die Anordnung der Erteilung von Verbindungsdaten, (der Grundrechtseingriff) muss hinreichend bestimmt sein.

a) Grundsatz (Abs. 1 Satz 1)

Gemäß § 100h I 1 StPO ist eine Anforderung grundsätzlich nur zulässig, wenn sie folgende Informationen über den Betroffenen enthält:

---

[103] BK/Badura, Art. 10, Rn 55; M/D/Herzog, Art. 10, Rn 56; AK/StPO/Maiwald § 100a, Rn 19; BGH, NJW 1993, 1212 (1213); OLG Hamm, Beschl. v. 29.07.1999 – 3 Ws 368/99; Berlin, Beschl. v. 12.04.1999 – 14 Qs 133/99; LG Bremen, StV 1999, 307.

[104] z.B. LG München I, NStZ-RR 1999, 85; OLG München, MMR 1998, 613f; aA: LG Bremen, StV 1999, 307; OLG Celle, StV 2000, 70.

[105] BGHSt 31, 296, 297.

- Name und Anschrift
- Rufnummer oder eine andere Kennung des TK-Anschlusses
- Art, Umfang und Dauer der Maßnahme (§ 100h I 3 i.V.m. § 100b II 3 StPO)

Der Grundrechtseingriff soll damit messbar und berechenbar sein[107].

b) Ausnahme (Abs. 1 Satz 2)

Liegt aber eine „Straftat von erheblicher Bedeutung" (s.o.) vor und ist anderenfalls eine Sachverhaltserforschung „aussichtslos oder wesentlich erschwert", genügt eine räumlich und zeitlich hinreichende Bestimmung über die Auskunft, die erteilt werden soll (vgl. § 100h I 2 StPO)[108]. Das heißt, Auskünfte über Verbindungsdaten von unbekannten Tätern, die eine Straftat mittels Endeinrichtung begangen haben, dürfen nur angeordnet werden, wenn auch eine Straftat von erheblicher Bedeutung vorliegt (s.o.)[109]. Durch diese Regelung werden auch „Funkzellenabfragen" bei Ermittlungen gegen einen namentlich unbekannten Täter vom Gesetz erfasst.

2. Form der Anordnung (§ 100h I 3 StPO)

Im Gegensatz zu § 12 I 1 FAG schreibt § 100h I 3, 1. HS i.V.m. § 100b II 1 StPO vor, dass eine Anordnung *schriftlich* zu erfolgen hat. Eine (fern-)mündliche Anforderung gegenüber dem TK-Unternehmen soll dann ausreichend sein, wenn die schriftlichen Unterlagen nachgereicht werden. Dem TK-Unternehmen ist eine Ausfertigung der Anforderung oder eine beglaubigte Kopie, die dessen Urheber erkennen lässt, zuzuleiten[110].

3. Eingriffskompetenz (§ 100h I 3 i.V.m. § 100b I StPO)

§ 100h StPO verweist bezüglich der Eingriffskompetenz auf die Bestimmungen über die Telekommunikationsüberwachung „entsprechend".

a) Regel-Kompetenz, Richtervorbehalt

Eine Auskunftserteilung darf grundsätzlich nur durch einen Richter angeordnet werden. Im Ermittlungsverfahren ist dies der Ermittlungsrichter.

Bereits bei der Anordnung des strafprozessualen Grundrechteingriffs soll ein Richter entscheiden, da der Betroffene in der Regel vorher nicht angehört wird (Modell des präventiven Rechtsschutzes[111]). Eine unabhängige Instanz soll die Anordnung überprüfen[112].

---

[106] Vgl. BT-Drs. 14/7008, S. 7; Eisenberg, Beweisrecht der StPO, Spezialkommentar, Rn 2450g.
[107] Wollweber, NJW 2002, 1554 (1555).
[108] Zu den Problemen der Auslegung siehe: LG Köln, Beschl. v. 15.1.2002 - 503 Gs 135/02; LG Wuppertal, Beschl. v. 13.2.2001 - 30 Qs 5/02.
[109] Entgegen dem Willen des Gesetzgebers, BT-Drs. 14/7008, S. 6 (7).
[110] AK/StPO/Amelung § 100, Rn 34.
[111] s. § 33 IV StPO, Ausnahme von der Anhörung; Welp, S. 56.
[112] Zu den strukturellen Defiziten des Richtervorbehalts: Paeffgen, in Rieß-FS, S. 413 (422-426).

b) Ausnahme-Kompetenz

Ausnahmsweise, bei Gefahr im Verzug, ist auch die Staatsanwaltschaft zur Anordnung befugt[113] (vgl. § 100b I 2 StPO).

Gefahr im Verzug liegt vor, wenn der Erfolg der Anordnung - verzögert durch die richterliche Entscheidung - gefährdet wäre[114].

Hinsichtlich der Auskunftserteilung über Verbindungsdaten der Vergangenheit ist Gefahr im Verzug anzunehmen, wenn die Datenlöschung bei den TK-Unternehmen nach Ablauf der Speicherfrist bevorsteht oder wenn anzunehmen ist, dass eine Auskunft für weitere unaufschiebbare Ermittlungsmaßnahmen benötigt wird[115].

Eine Anordnung durch die Staatsanwaltschaft bei Gefahr im Verzug tritt jedoch außer Kraft, wenn nicht ein Richter diese binnen drei Tagen bestätigt. Damit werden Maßnahmen mit Dauerwirkung einer richterlichen Kontrolle unterworfen.

c) Befristung

§ 100h I 3 HS 2 StPO ordnet an, dass § 100b II 4, 5, IV StPO entsprechend gilt. Eine Anforderung hinsichtlich zukünftiger Verbindungsdaten ist damit auf 3 Monate befristet. Die Anforderung soll nicht zu einem unbefristeten Grundrechtseingriff führen.

Jedoch ist es möglich, Auskunftsverlangen um jeweils weitere maximal drei Monate zu verlängern, aber nur soweit die Voraussetzungen erfüllt sind (vgl. § 100b II 4, 5 StPO entsprechend).

4. Eingriffsverbote, Beweisverbote

Nach § 12 I 1 FAG gab es keine Verbote, in geschützte Rechtsgüter einzugreifen. Eingriffsverbote sind auch heute weder für die TK-Überwachung noch allgemein für heimliche Maßnahmen gesetzlich geregelt[116].

Als neu eingefügte Norm enthält § 100h StPO in Absatz 2 Satz 1 ein Verbot des Eingriffs in geschützte Rechte.

a) Beweiserhebungsverbot

Soweit ein Zeugnisverweigerungsrecht (ZV-Recht) nach § 53 I 1 Nr. 1, 2, 4 StPO reicht, ist eine Auskunfts-Anforderung unzulässig. Ist ein ZV-Berechtigter (Geistlicher, Verteidiger, Abgeordneter) an der TK beteiligt, darf eine Auskunft über die Verbindungsdaten nicht eingeholt werden (§ 100h II 1 HS 1 StPO). Werden dennoch Aus-

---

[113] Nicht befugt sind Hilfsbeamte der Staatsanwaltschaft; Malek/Wohlers, Rn 432.

[114] Vgl. BVerfGE 51, 111 = NJW 1974, 1540; jüngst für Art. 13 GG: „Gefahr in Verzug“ eng auszulegen, BVerfG NJW 2001, 1127; dazu Amelung, NStZ 2001, 337.

[115] Welp, S. 57.

[116] BGHSt 19, 325 (329); 31, 304 (307); Wolter, in Rieß-FS, S. 633 (635); Ausnahme: „großer Lauschangriff“, § 100 d III StPO.

künfte erlangt, ist eine Verwertung ausgeschlossen (§ 100h II 1 HS 2 StPO).

Mit der Einfügung eines Beweiserhebungsverbotes für Verbindungsdaten bleibt die umfassendere Telekommunikationsüberwachung (§ 100a f. StPO) als stärkerer Grundrechtseingriff ohne eine solche Regelung[117].

Ausdrücklich geschützt sind nur Parlamentarier, Geistliche und Strafverteidiger. Kritisiert wird, dass Journalisten nicht zu den privilegierten Funktionsträgern zählen, obwohl der Presse „als Wesenselement des freiheitlichen Staates [...] unentbehrlich“[118] ist.

Von § 100h II 1 Alt. 1 StPO sind ebenfalls auch nicht die Berufshelfer der genannten Funktionsträger erfasst (geschützt durch § 53a I S. 1, 97 IV StPO).

b) Verfassungsrechtliche Eingriffs- und Verwertungsverbote

Hinsichtlich der Pressefreiheit können sich, obwohl nicht in § 100 h II 1 HS 1 StPO genannt, Einschränkungen des Auskunftsrechts ergeben, wenn z.B. Journalisten an der Telekommunikation beteiligt sind[119]. Die Pressefreiheit (Art. 5 I 2 GG), besonders die Geheimhaltung von Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informant, ist bei Speicherung, Verwertung und Weitergabe von Verbindungsdaten zu beachten[120]. Journalisten sind gem. § 53 I S. 1 Nr. 5, S. 2 StPO berechtigt über die Person eines Informanten und dessen Mitteilungen das Zeugnis zu verweigern. Dies gilt aber nur für redaktionelle Arbeit (Abs. 1, Satz 3). Ausnahmen von diesem Recht ergeben sich aus § 52 II 2 StPO. Eine Rückausnahme ergibt sich, wenn die Aussage zur Offenbarung der Person des Informanten führen würde (§ 53 II 3 StPO).

Mit einer Verfassungsbeschwerde wehren sich nun Journalisten gegen ihre Instrumentalisierung durch die Strafverfolgungsbehörden. Verbindungsdaten von Journalisten, die in Kontakt mit den Flüchtigen standen, führten zur Feststellung der Aufenthaltsorte und Festnahme des RAF-Terroristen Hans-Joachim Klein und des Kreditbetrügers Jürgen Schneider[121].

c) Verwertungsverbote (§ 100h II 1, 2. HS StPO)

Wird eine durch § 100h II 1 HS 1 i.V.m. § 53 I 1 Nr. 1, 2, 4 StPO unzulässige Erlangung einer Auskunft dennoch erlangt, darf sie nicht verwendet werden (2. Halbsatz). Damit wird klargestellt, dass eine unzulässige Auskunftsanordnung nicht zu einer zulässigen Verwertung führen kann.

---

[117] Zum Bewertungswiderspruch: Welp, GA 2002, 535 (547); SK/Wolter, § 100g, Rn 2.
[118] BVerfGE 20, 162; 52, 283 (296); Welp, GA 2002, 535 (549).
[119] Welp, S. 60, 61; Stichwort: Informanten.
[120] Vgl. BVerfGE 50, 234 (240); 66, 116 (130 ff.); 77, 65 (74 f.); LG Frankfurt, NJW 1996, 1008;
[121] Verfassungsbeschwerde „Stern“/ZDF : 1 BvR 330/96, mündliche Verhandlung 20.11.02; Urteil in einigen Wochen.

5. Entprivilegierung (§ 100h II 2 StPO)

Anders ist dies jedoch, wenn die zur Zeugnisverweigerung Berechtigten einer Teilnahme oder Begünstigung, Strafvereitelung oder Hehlerei verdächtig sind. Ein Verlangen der Strafverfolgungsbehörden, Auskunft über Verbindungsdaten zu erteilen, ist dann unter den in § 100h II 2 StPO genannten Voraussetzungen zulässig.

Problematisch ist, ob die Verbindungsdaten des Strafverteidiger bei Beteiligung an der Tat erhoben und verwertet werden können, da sich nach Meinung des BGH der Strafverteidiger auch bei Verdacht der Begehung einer Anschluss-Tat auf das Recht auf freien Verkehr mit dem Beschuldigten (§ 148 StPO) berufen kann[122].

6. Zufallsfunde, Verwendung von VD in anderen Verfahren (§ 100h III StPO)

§ 12 FAG sah keine Beschränkungen der Verwertbarkeit von Auskünften vor. Ein so genannter Zufallsfund war gemäß § 108 StPO verwertbar.

§ 100 h Absatz 3 StPO sieht vor, dass erlangte personenbezogene Informationen in anderen Verfahren nur verwendet werden dürfen, soweit der Beschuldigte zustimmt oder sich Erkenntnisse ergeben, „die zur Aufklärung einer in § 100g I 1 StPO genannten Straftat benötigt werden [...]."

7. Löschungspflicht (§ 100h I 3 StPO)

§ 100h I 3 HS 2 StPO verweist entsprechend auf die Bestimmung in § 100b VI StPO. Der datenschutzrechtliche Grundsatz der Zweckbindung erhobener Daten (Art. 2 I iVm. Art. 1 I GG[123]) beinhaltet die Pflicht, durch die Anordnung erlangte, zur Strafverfolgung nicht mehr erforderliche Unterlagen, unverzüglich unter Aufsicht der Staatsanwaltschaft zu vernichten, wobei eine Niederschrift anzufertigen ist (§ 100h I 3 HS 1 i. V. m. § 100b VI StPO). Durch diese Regelung verpflichtet sind nur die Justizbehörden. Die Fristen für die Speicherung von Verbindungsdaten bei den TK-Unternehmen (§ 7 III, IV TDSV) bleiben unangetastet.

8. Mitteilungspflicht (§ 101 I 1 StPO)

§ 101 StPO regelt die Benachrichtigung der durch Eingriffe Betroffenen.

Mit Einfügung der §§ 100g, h StPO nennt § 101 StPO auch die Bestimmungen über die Auskunftserteilung. Die Beteiligten sind zu benachrichtigen, „sobald dies ohne Gefährdung des Untersuchungszwecks, der öffentlichen Sicherheit, von Leib und Leben einer Person sowie der weiteren Verwendung eines eingesetzten nicht offen ermittelnden

[122] BGHSt 33, 347 ff.; eingehend: Welp, GA 2002, 535 (551) m.w.N.

[123] BVerfGE 65, 1 (42, 45); 80, 367 (373); AK/GG/Bizer, Art. 10, Rn 64; geschützt: der Informations- und Datenverarbeitungsprozess (vgl.o.).

Beamten geschehen kann."[124]

a) Heimlichkeit und rechtliches Gehör

Zweck der Mitteilungspflicht ist es, die regelmäßig vorher nicht angehörten Betroffenen über den Grundrechtseingriff zu informieren und ihnen nachträglich rechtliches Gehör zu verschaffen[125].

Nachdem der Zweck des Eingriffs erreicht ist, soll im Rechtsstaat Transparenz über das Handeln der staatlichen Ermittlungsorgane hergestellt werden.

Einschlägig könnten hier der Anspruch auf rechtliches Gehör (Art. 103 I GG) und die Rechtsschutzgarantie (Art. 19 IV 1 GG) sein. Nur diejenigen, die über den Eingriff Kenntnis haben, können sich dagegen auch wehren.

Das Bundesverfassungsgericht erkennt einen Anspruch auf Benachrichtigung bereits aus der Gewährleistung des TK-Geheimnisses (Art. 10 GG)[126].

b) Beteiligte - Zielwahlsuche

Beteiligte i.S. des § 101 I 1 StPO sind die von den Maßnahmen unmittelbar Betroffenen (z.B. der Beschuldigte[127] und Nachrichtenmittler). Zu benachrichtigen sind die Personen, die in ihrer Rechtsposition verletzt sein können[128].

Bei einer Zielwahlsuche werden millionenfach Datensätze abgeglichen, es kommt zu ebenso vielen Eingriffen. Jeder vom Eingriff Betroffene müssten eigentlich informiert werden. Denn auch eine Negativauskunft über die Telekommunikation ist vom Fernmeldegeheimnis geschützt. Hier sieht das Bundesverfassungsgericht es jedoch als genügend an, wenn eine unabhängige Kontrollinstanz - z.B. ein Kontrollausschuss des Bundestages (vgl. Art. 10 II 2 GG) oder ein Datenschutzbeauftragter - eingeschaltet wird[129].

VI. Rechtsschutz

Das Auskunftsersuchen untersteht der Rechtsschutzgarantie des Art. 19 IV 1 GG (Recht auf effektiven und möglichst lückenlosen gerichtlichen Rechtsschutz)[130]. In der Vergangenheit war dies in einer differenzierten Betrachtung umstritten.

1. Gegen die Auskunfts-Anforderung

a) Anforderung durch den Richter

Ordnet ein Richter die Auskunftserteilung an und ist der Eingriff noch nicht erledigt, so

---

[124] Dies ergibt sich bereits aus der Verfassung: BVerfG, Beschl. v. 14.7.1999, Abs.Nr. 169, 170, 1 BvR 2226/94, www.bverfg.de.
[125] BGHSt 36, 311; SK/Rudolphi/Wolter, § 101, Rn 1; Pfeiffer StPO § 101, Rn 1.
[126] BVerfG, NJW 2000, 55, 57; BVerfGE 30, 1 (17 ff., 31).
[127] SK/StPO/Rudolphi § 100, Rn 14; aA Pfeiffer StPO § 100b, Rn 6.
[128] h.L.; BGHSt 7, 153; 13, 75 (77); Meyer-Goßner, Vor § 296, Rn 9.
[129] BVerfGE 65, 1 (60); BVerfG, v. 14.7.1999, Abs. Nr. 169, 170, 1 BvR 2226/94, www.bverfg.de.
[130] Gusy, StV 2002, 153 (157).

besteht das Rechtsmittel der Beschwerde gemäß §§ 304 ff. StPO, die auf die Aufhebung der Anordnung gerichtet ist[131].

b) Anforderung durch die Staatsanwaltschaft

Ungeregelt ist dagegen der Rechtsschutz bei staatsanwaltschaftlicher Anforderung. Streitig ist, ob die §§ 23 ff. EGGVG oder § 98 II 2 StPO analog anzuwenden sind.

Die Literatur vertritt die Auffassung, dass die §§ 23 ff. EGGVG auch auf strafprozessuale Grundrechtseingriffe anwendbar sind[132].

Ein solches Verfahren ist jedoch nach den §§ 23 ff. EGGVG gegenüber spezialgesetzlichen Regelungen subsidiär (§ 23 III EGGVG). Daher kommt im Rahmen eines Strafverfahrens eine analoge Anwendung von § 98 II 2 StPO in Betracht. Es müsste eine planwidrige Regelungslücke bestehen. Ein Rechtsschutz gegen Anordnungen der Staatsanwaltschaft existiert nur für die Beschlagnahme (§ 98 II 2 StPO).

Planwidrig ist die Regelungslücke, weil der Gesetzgeber bei Verabschiedung der StPO (weit vor dem Grundgesetz) eine Rechtsschutzgarantie nicht berücksichtigt hat.

§ 98 II 2 StPO ermöglicht dem Richter, eine nachträgliche Entscheidung über den Eingriff zu treffen.

Die herrschende Auffassung in Rechtsprechung und Literatur bejaht auf Grund einer vergleichbaren Interessenlage eine analoge Anwendung des § 98 II 2 StPO auf alle Eileingriffe der Staatsanwaltschaft[133] und damit auch auf die Anordnung von Verbindungsdaten. § 100h I 3 StPO i.V.m. § 100b I 3 StPO ordnet aber ohnehin innerhalb von drei Tagen eine richterliche Bestätigung an.

2. Gegen erledigte Anforderungen

a) Erledigung des Auskunftsersuchens

Wann ein strafprozessualer Eingriff erledigt ist, ist streitig. Es wird die Auffassung vertreten, dass ein Eingriff erst erledigt ist, wenn Neben- und Folgewirkungen weggefallen sind, d. h. keine Beschwer mehr vorliegt[134].

Es lässt sich bei der Erledigung aber auch auf das Rechtsschutzziel des Betroffenen abstellen[135].

Bei der Auskunftserteilung und Telekommunikationsüberwachung kann die Erledigung

---

[131] Welp, S. 66.

[132] Schenke NJW 1976, 1816 (1818 ff.); Meyer-Goßner EGGVG § 23, Rn 10; a.A. OLG Karlsruhe NJW 1976, 1417 (1418); OLG Stuttgart NJW 1977, 2276; Jorzig/Kunze, Jura 1990, 294 f.

[133] OLG Stuttgart, NJW 1977, 2276; BGHSt 36, 30 (31); Dähn, JA 1981, 7 (10); AK/StPO/Amelung § 98, Rn 27, § 100, Rn 29; weitere Verweise: Welp, S. 68, 69.

[134] Folgewirkungen: Karl Peters, JR 1973, 341; Beschwer: OLG Frankfurt, GA 1980, 29 (30).

[135] Amelung, Rechtsschutz, S. 44; Schenke, Jura 1980, 133 (134); Welp, S. 69.

in der Beendigung der Überwachung[136] bzw. in der Auskunftserteilung oder in der Vernichtung der Unterlagen[137] gem. § 100b VI StPO zu sehen sein.

Da in der Verwertung des Eingriffs ebenfalls ein Eingriff zu sehen ist (s.o.), kann eine Erledigung erst mit der Vernichtung der den Eingriff aufrecht erhaltenden Unterlagen vorliegen.

b) Anforderung durch den Richter

Streitig in Rechtsprechung und Literatur war, ob ein Beschwerdeverfahren gem. §§ 304 ff. StPO auch bei erledigten strafprozessualen Eingriffen Anwendung finden sollte. Die Rechtsprechung bis zum BVerfG lehnte zunächst eine Beschwerde gegen eine richterliche Zwangsmaßnahme ab[138].

Eine Mindermeinung wollte aus der Rechtsschutzgarantie oder aus dem Grundsatz des rechtlichen Gehörs eine Beschwerdebefugnis herleiten. Das Bundesverfassungsgericht ist 1997 der Mindermeinung gefolgt[139]. Danach sind strafprozessuale Feststellungsbeschwerden statthaft. Bei einem „tiefgreifenden Grundechtseingriff" besteht ein Feststellungsinteresse. Der strafprozessuale Rechtsschutz darf nicht deshalb unzulässig sein, weil der Eingriff vollzogen und daher erledigt sei[140].

c) Anforderung durch den Staatsanwalt

Die herrschende Auffassung hinsichtlich durch die Staatsanwaltschaft angeordneter erledigter Grundrechtseingriffe bejaht ein Rechtsschutzverfahren gem. § 98 II 2 StPO analog, da bei bevorstehenden Eingriffen eine analoge Anwendung ebenfalls zulässig ist. Oder aber die Norm wird verfassungskonform ausgelegt[141]. Der sachnähere § 98 II 2 StPO ist § 28 I 4 EGGVG vorzuziehen.

C. Verfassungsmäßigkeit der §§ 100g, h StPO

Die Grundrechte aus Art. 10 I und Art. 2 I i.V.m. Art. 1 I GG (Fernmeldegeheimnis und informationelle Selbstbestimmung) sind durch die Anforderung von Verbindungsdaten betroffen. Dieser Grundrechtseingriff ist verfassungsmäßig, wenn er verfassungsrechtlich gerechtfertigt ist.

I. Verfassungsrechtliche Rechtfertigung der §§ 100g, h StPO

Ein Eingriff ist verfassungsrechtlich gerechtfertigt, wenn er auf einer verfassungsmäßigen

---

[136] Schnarr, MDR 1987, 1 (5).; Welp, S. 69.
[137] Welp, Überwachung, S. 116; Malek/Rüping, Zwangsmaßnahmen, S. 133, Rn 258.
[138] BGHSt 10, 88 (91); 36, 30 (32); BGH NStZ 1989, 538; AK/StPO/Wassermann, § 81a, Rn 12; KK/StPO, § 98, Rn 24; Meyer-Goßner, Vor StPO § 296, Rn 17 f.
[139] Amelung, Rechtsschutz, S.57 ff.; BVerfG NJW 1997, 2163 ff; BVerfG, EuGRZ 1997, 372 ff, 374 ff.; BVerfG, NJW 1998, 2131 f.
[140] BVerfGE 96, 27, Leitsatz 2; Gusy, StV 2002, 153 (157); Amelung, StV 2002, 161 (163).
[141] Analoge Anwendung: BGH, NJW 1978, 1013; BGHSt 36, 30; Amelung, Rechtsschutz, S. 49 ff.; verfassungskonforme Auslegg.: Rieß/Thym, GA 1981, 189 (203 ff.); Jorzig/Kunze, Jura 1990, 294, 298.

gesetzlichen Grundlage beruht.

1. Gesetzgebungsverfahren

Ein Grundrechtseingriff bedarf einer gesetzlichen Grundlage (Vorbehalt des Gesetzes). Eingriffsgrundlage sind §§ 100g, h StPO.

Der Erlass der Eingriffsgrundlage ist hinsichtlich Zuständigkeit, Verfahren und Form nicht zu beanstanden. Die Bund hat gemäß Art. 72, 74 Nr. 1 GG die Kompetenz zur Gesetzgebung im Bereich des Strafrechts und des gerichtlichen Verfahrens[142].

Die Bundesregierung hat den Gesetzentwurf[143] am 01.10.2001 im Bundestag eingebracht (Art. 76 I Alt. 1 GG) sowie 3 Wochen zuvor (07.09.2001) die Vorlage dem Bundesrat gem. Art. 76 I 1 GG als besonders eilbedürftig zugeleitet (Art. 76 II 4 GG). Nach Äußerung des Bundesrates und Gegenäußerung der Bundesregierung zum Entwurf (19.10. und 01.11.2001[144]) gab der Rechtsausschuss am 28.11.2001 eine Beschlussempfehlung ab (Art. 77 I 1 GG). Die Neuregeung wurde im Bundesgesetzblatt verkündet (Art. 82 GG) und trat am 01.01.2002 in Kraft.

2. Vorbehalt des Gesetzes, Ermächtigungsgrundlage

a) Anforderung von Verbindungsdaten

Die Anforderung von Verbindungsdaten regeln die §§ 100g, h StPO (s.o.).

b) Zielwahlsuche

aa) Zulässigkeit der Beschaffung von Informationen

§ 100g II StPO regelt die Auskunftserteilung von Zielwahlsuche-Ergebnissen an die Strafverfolgungsbehörden. Fraglich ist jedoch, ob die TK-Unternehmen (diejenigen, die geschäftsmäßig TK-Dienste erbringen) überhaupt befugt sind, Dateien-Abgleiche durchzuführen und Daten weiterzugeben.

- Gemäß § 85 III 1 TKG ist es den TK-Unternehmen untersagt, über die Kommunikation Kenntnis zu nehmen, soweit sie nicht der geschäftsmäßigen Erbringung von TK-Dienstleistungen, z.B. der Entgeltabrechnung[145], dient.

Die Kenntnisnahme von Datensätzen bestimmter einzelner Anschlüsse ist zulässig (s.o.), da beim Anrufenden eine Entgeltabrechnung erfolgt.

- Durch die Zielwahlsuche werden jedoch die Verbindungsdaten aller Anschlüsse mit der Anschlussnummer des Opfers/Täters abgeglichen.

bb) § 100g II StPO – Anforderung; keine Ermächtigung zum Datenabgleich

Dieser Abgleich aller Verbindungsdatensätze ist nicht von § 85 III 1 TKG gedeckt. Die Zielwahlsuche als „spezifische kriminalistische“ Ermittlungsmethode ist für die Erbringung von TK-Dienstleistungen nicht notwendig[146].

Durch § 100g StPO lasse sich lediglich eine Auskunft anfordern, die die TK-Unternehmen

---

[142] Paeffgen, in Roxin-FS, 413 (419f).
[143] BT-Drs. 14/7008.
[144] BR-Drs. 702/01 und BT-Drs. 14/7258; BT-Drs. 14/7679.
[145] Beck‘scher TKGK/Büchner, § 85, Rn 6.

(durch eine Zielwahlsuche) erlangen.

Bereits § 12 FAG enthielt nur eine Anforderungsermächtigung und ermächtigte die TK-Unternehmen nicht zur Datenerhebung durch eine Zielwahlsuche[147].

Eine ausdrückliche Rechtsgrundlage für den Abgleich von Verbindungsdaten zum Zwecke der Erteilung einer Auskunft i.S.d. § 100g II StPO existiert nicht[148].

Eine solche Grundlage zum Datenabgleich existiert nur z.B. zur Aufdeckung von Telekommunikationsmissbrauch i.S. der §§ 89 II Nr. 1e TKG i.V.m. § 7 II 1, § 8 I TDSV.

Nach Meinung von Welp und Weßlau wurde das Problem einer mangelnden Grundlage in der Literatur noch nicht erkannt[148].

cc) § 100g II StPO als Ermächtigungsgrundlage

Wolter[149] meint, dass sich aus der ausdrücklichen Zulassung der Zielwahlsuche in § 100g II StPO auch die Durchführung dieser Maßnahme ergibt, wenn Dritte unvermeidbar betroffen werden. Der Gesetzgeber habe im Gegensatz zu § 100c III, 163f II StPO, aber im Einklang mit § 100a StPO den Eingriff nicht ausdrücklich geregelt.

3. Einschränkung der Grundrechtsbeschränkung

Der Eingriff in Grundrechte wird dadurch begrenzt, dass der Eingriff an sich bestimmt und verhältnismäßig sein muss.

a) Zitiergebot, Art. 19 I 2 GG

Durch die Anforderung der Verbindungsdaten der Telekommunikation wird in den Art. 10 I GG eingegriffen. Das eingreifende Gesetz kann nur dann verfassungsrechtlich gerechtfertigt sein, wenn es das eingeschränkte Grundrecht unter Angabe des Artikels nennt[150].

§ 12 FAG enthielt in Satz 2 den Hinweis auf das eingeschränkte Grundrecht des Art. 10 I, Alt. 3 GG. Das Zitiergebot wird bei § 100g StPO dadurch beachtet, das in Art. 3 des Gesetzes zur Änderung der Strafprozessordnung vom 20.12.2001 Art. 10 I GG als betroffenes Grundrecht genannt wird.

Unter anderem beim Recht auf informationelle Selbstbestimmung verzichtet das Bundesverfassungsgericht auf das Zitiergebot, sodass hier die Eingriffsnorm nicht auf Art. 2 I i.V.m. Art. 1I GG aufmerksam machen muss[151].

b) Bestimmtheitsgebot, rechtliche Klarheit

Die §§ 100g, h StPO könnten dem verfassungsrechtlichen Bestimmtheitsgebot genügen. Der Regelungsgehalt darf nicht unverständlich sein[152].

Die §§ 100g f. StPO regeln die Anforderung von Verbindungsdaten durch die Strafverfolgungs-

---

[146] Lediglich Übermittlungs- keine Ermittlungsbefugnis der TK-Unternehmen, Welp, S. 102.
[147] Siehe: Welp, S. 100-102; Weßlau, ZStW 2001, 693.
[148] Zu § 12 FAG: Welp, S. 102; Weßlau, ZStW 2001, 693; a.A. Pfeiffer StPO, § 100g, Rn 5.
[149] SK/Wolter, § 100g, Rn 16; Pfeiffer StPO, § 100g, Rn 5.
[150] Pieroth/Schlink, Rn. 310.
[151] Dreier, Grundgesetz, Kommentar, Art. 19 I, Rn 18 ff.
[152] BVerfGE 65, 1 (65); 100, 313 (360).

behörden. Diejenigen Verbindungsdaten, die angefordert werden können, sind abschließend aufgezählt, die betroffenen Personen in §§ 100g, h StPO genannt. Die Regelung der Auskunftserteilung ist daher im Gegensatz zu § 12 FAG rechtlich klar und bestimmt.

c) Verhältnismäßigkeit des Gesetzes

Der gesetzliche Eingriff in Grundrechte könnte auch verhältnismäßig sein, wenn er einem legitimen Zweck dient und geeignet, erforderlich und angemessener ist.

aa) Legitimer Zweck: Der Zweck der Anordnung ist die Sicherung von Beweismitteln, die der Ermittlung der Wahrheit und der Verbrechensbekämpfung dient. Die wirksame Strafverfolgung (s.o.) ist ein legitimer Zweck.

bb) Geeignetheit: Es ist aber auch zu fragen, ob die Anordnung der Maßnahme auch geeignet ist, dem legitimen Zweck zu dienen. Durch Beweismittel wird ein Sachverhalt aufgeklärt und die Wirksamkeit der Strafverfolgung sichergestellt. Dahingehend sind die §§ 100g, h StPO zweckdienlich und geeignet.

cc) Erforderlichkeit: Die Auskunftserteilung ist notwendig, wenn es kein milderes gleich wirksames Mittel gibt. Eine umfassende TK-Überwachung ist schon nicht milder.

(1) „Einfache" Anforderung, bekannter Tatverdächtiger

Gemäß § 100g I 1 StPO darf Auskunft von Verbindungsdaten nur angeordnet werden, wenn sie zur Untersuchung notwendig ist. Es wird damit auf das Verhältnismäßigkeitsprinzip verwiesen.

(2) Funkzellenabfrage bei Ermittlung gegen unbekannt, § 100h I 2 StPO

Die Anforderung von räumlich und zeitlich hinreichend bestimmten Daten aus dem Datenbestand einer in einer Funkzelle angefallenen Telekommunikation ist nur zulässig, wenn andernfalls die Sachverhaltserforschung aussichtslos oder wesentlich erschwert wäre.

Diese Subsidiaritätsklausel genügt dem Gebot der Erforderlichkeit und stellt eine höhere Schwelle an die Anforderung dar als die „einfache" Auskunftserteilung, da eine gewisse Anzahl von Verbindungsdaten Unbeteiligter von den Strafverfolgungsbehörden erfasst werden.

(3) Zielwahlsuche, § 100g II StPO

Auch die Zielwahlsuche könnte erforderlich sein. § 100g II StPO schafft eine gesetzliche Grundlage für die Auskunft über TK-Verbindungsdaten, die durch eine Zielwahlsuche gewonnen werden. § 12 I 1 FAG sah nicht ausdrücklich eine Zielwahlsuche vor.

Die Zielwahlsuche kommt nach § 100g II StPO nur subsidiär zur Anwendung, es dürfen keine milderen gleich wirksamen Mittel zur Verfügung stehen.

Durch die Zielwahlsuche sollen die Anschlüsse ermittelt werden, über die z.B. mit dem Beschuldigten TK-Verbindungen bestanden haben. Abgesehen von den wenigen Verdächtigen sind mehrere Millionen Unbeteiligte betroffen. Es werden typischerweise bis zu 450 Millionen Datensätze abgeglichen[153]. Über die festgestellten Verbindungen (Treffer) dürfen die TK-Unternehmen gem. § 100g II i.V.m. § 100g I 2 StPO Auskunft erteilen, weil die Verbin-

[153] Welp, S. 103.

dungsdaten den Beschuldigten oder Nachrichtenmittler betreffen.

Für zukünftige Kommunikation kommt als milderes Mittel eine „Fangschaltung[154]“ (§ 89 II Nr. 3b TKG; § 10 I TDSV) auf Antrag des Opfers in Betracht, die nur den Täter und nicht millionenfach unbeteiligte betrifft.

dd) Angemessenheit: Die Regelung des § 100g StPO ist dann angemessen, wenn eine Abwägung dazu führt, dass das Recht der Allgemeinheit auf eine effiziente Strafverfolgung höher zu bewerten ist als das Recht des Einzelnen auf informationelle Selbstbestimmung und das Telekommunikationsgeheimnis.

(1) Bestimmter und bestimmbarer Täter, §§ 100g I, 100h I 2 StPO

Die Anforderung von Verbindungsdaten zur Sachverhaltserforschung und zur Ermittlung des Aufenthaltsortes des Täters ist bei namentlich bekannten Verdächtigen nur bei einer Straftat von erheblicher Bedeutung bzw. mittels einer Endeinrichtung möglich. Bei namentlich unbekannten ist mindestens eine erhebliche Straftat erforderlich.

Bereits § 100g f. StPO grenzt die Anforderung von VD ein. Damit ist die Auskunftserteilung bei Abwägung von Interessen des Täters (Art. 10 I Alt. 3, 2 I / 1 I GG) und der Allgemeinheit (wirksame Strafverfolgung) angemessen.

(2) Zielwahlsuche, Massengrundrechtseingriff

Der Eingriff durch § 100g II StPO könnte auch verhältnismäßig sein, d.h. nicht außer Verhältnis zu Gemeinwohlinteressen stehen[155].

Bedenklich ist die Zielwahlsuche hinsichtlich ihrer Intensität. Es ist zu Fragen wie viele Grundrechtsträger wie intensiv in ihren Grundrechten beeinträchtigt sind[156].

In der Bundesrepublik lassen sich alle Verbindungsdaten kontrollieren, soweit sie zur Entgeltberechnung nötig sind. Die Zielwahlsuche ist damit ein „Massengrundrechtseingriff“. Praktisch kann die gesamte Bevölkerung „abgeglichen“ werden[157].

Aufgrund der Reichweite der Zielwahlsuche darf eine Auskunft nur angeordnet werden, soweit der Verdacht einer in § 100g I StPO genannten Straftat besteht und wenn die Erforschung des Sachverhaltes oder die Aufenthaltsort-Ermittlung des Beschuldigten „auf andere Weise aussichtslos oder wesentlich erschwert wäre“ (§ 100g II StPO). Damit ähneln die Voraussetzungen der Zielwahlsuche denen der Telekommunikationsüberwachung. Hinsichtlich des § 12 FAG wurde die Zielwahlsuche wegen Unverhältnismäßigkeit als verfassungswidrig angesehen[158].

Bei der Eingriffsintensität wird die Zielwahlsuche auch mit der Rasterfahndung verglichen. Dem wird entgegengehalten, dass sich die Zielwahlsuche lediglich auf ein Kriterium, das der TK-Verbindungsdaten, beziehe und deshalb (weniger eingreifend) auch zulässig sei.

---

[154] Während des Verbindungsvorgangs werden die Verbindungsdaten des Anrufers übertragen; BVerfGE 85, 386 ff.

[155] BVerfG, NJW 2000, 55, 61.

[156] BVerfG, NJW 2000, 55, 61.

[157] Welp, S. 106, 107.

[158] Unverhältnismäßigkeit: Welp, S. 108.

Auch wenn eine Ermächtigungsgrundlage für eine Zielwahlsuche angenommen wird, ist sie trotz angehobener Eingriffsvoraussetzungen nicht verhältnismäßig. Eine bloße Subsidiaritätsklausel reicht nicht aus, um einen Massengrundrechtseingriff (ein Verdächtiger und rund 400 Millionen Grundrechtseingriffe) zu rechtfertigen.

II. Zusammenfassung, Stellungnahme

Mit der Neuregelung der Auskunftserteilung über Verbindungsdaten der Telekommunikation (§§ 100g, h StPO) wurde die – in § 12 FAG praktisch nicht vorhandene – Eingriffsschwelle insoweit auf ein verfassungsrechtlich nicht zu beanstandendes Maß angehoben, als sie die Anforderung von VD eines bekannten Täters oder auch eines unbekannten Täters betrifft, wenn zumindest dessen TK räumlich und zeitlich bestimmbar ist.

Der strafprozessuale Grundrechtseingriff ist nur bei Straftaten von erheblicher Bedeutung oder, wenn der Täter hinreichend bestimmt ist, auch bei Straftaten mittels Endeinrichtung möglich und verfassungsmäßig.

Die Durchführung der eingriffsintensiven Zielwahlsuche ist an sich nicht ausdrücklich geregelt. § 100g II StPO (als Norm für den Auskunftsanspruch einer durchzuführenden Zielwahlsuche) wird der Intensität des Grundrechtseingriffs nicht gerecht.

M. E. ist der Deliktskatalog für die Zielwahlsuche zu weit. Ein millionenfacher Grundrechtseingriff durch die Datenabgleichung ist nicht angemessen im Verhältnis zur Verfolgung z.B. eines Einbruchsdiebstahls als erhebliche Straftat i.S. des § 100g StPO.

D. Ausblick, Vorratsspeicherung

Die Pflicht zur Auskunftserteilung besteht nur bei legal gemäß der TDSV erhobenen Verbindungsdaten. Die TK-Betreiber sind danach nicht verpflichtet, Verbindungsdaten zu speichern. Bei Pauschalentgelten (sog. Flat-Rates bei DSL[159]) oder kostenlosen TK-Angeboten entstehen grundsätzlich keine VD, die Gegenstand einer Auskunftspflicht sein könnten[160].

Auf europäischer und nationaler Ebene wird aber eine Vorratsspeicherung jeglicher Daten der Telekommunikation (und der Teledienste) erwogen[161].

Eine solche Speicherung auf Vorrat zu einem noch nicht bestimmten/ bestimmbaren Zweck ist im Hinblick auf das Recht auf informationelle Selbstbestimmung (s. Volkszählungsurteil) äußerst kritisch zu sehen.

---

[159] Digital Subscriber Line; Modulationsverfahren für die Übertragung von Informationen über das herkömmliche Telefon-Festnetz.

[160] Weßlau, ZStW 113 (2001), 681 (701); Welp, GA 2002, 535 (556).

[161] BR-Drs. 14/9801, S. 8; Amtsblatt der Europäischen Gemeinschaften, 31.07.02, L201/37-L201/47: Richtlinie 2002/58/EG, vom 12.Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatspähre in der Kommunikation (*Datenschutzrichtlinie für die elektronische Kommunikation*); Diskutiert auch auf der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Mainz, 25.10.2002.

E. Exkurs: IMSI-Catcher

I. Verbindungsdaten: § 100i StPO – Der IMSI-Catcher

Durch die mobile Kommunikation lässt sich - anders als beim Festnetz – nicht mehr ohne weiteres vom Aufenthaltsort eines Mobilfunkbenutzers auf die Anschlusskennung schließen[162].
Das Bundeskriminalamt (BKA) und der BGS setzen seit 1998 in Fällen besonders schwerer Kriminalität sog. „IMSI-Catcher“ ein, um Lücken in den polizeilichen Eingriffsmöglichkeiten zu schließen[163].
Bereits 1997 wollte der Bundesrat eine Ermächtigungsgrundlage für den Einsatz dieses Gerätes schaffen[164]. Dazu kam es jedoch nicht.
Ein Pressebericht war Ausgangspunkt für eine Kleine Anfrage[165] der FDP-Fraktion, ob die Bundesregierung u.a. den Einsatz eines sog. IMSI-Catchers durch die Strafverfolgungsbehörden als von § 100a StPO gedeckt ansehe.
Mit Verabschiedung des Terrorismusbekämpfungsgesetzes[166] wurden bereits der Bundesverfassungsschutz und der MAD zur Nutzung des IMSI-Catchers ermächtigt.

II. Funktion des IMSI-Catchers

Mit Hilfe eines sog. IMSI-Catchers ist es möglich, die IMSI und IMEI zur ermitteln[167], sowie einen Mobilfunk-Nutzer (dessen Mobilfunkgerät sich im Stand-By-Modus befindet) zu lokalisieren. Eine Weiterentwicklung des ursprünglichen Gerätes erlaubt auch das Abhören abgehender Gespräche.
Der IMSI-Catcher simuliert eine Basisstation eines Mobilfunknetzes. Alle eingeschalteten Mobilfunkgeräte im Einzugsbereich des Catchers buchen sich bei diesem ein. Dadurch lassen sich die IMSI und IMEI gewinnen. Der Catcher arbeitet mit einer Leistung von weniger als einem Watt, womit die Funkzellenausdehnung gering und eine Einschränkung des Aufenthaltsortes ermöglicht wird[168].

III. Regelung des § 100i StPO

Mit dem Gesetz zur Änderung der Strafprozessordnung vom 6. August 2002[169] wurde nun durch Einfügung des neuen § 100i StPO der Einsatz des IMSI-Catchers auch im Ermittlungsverfahren ausdrücklich zugelassen, obwohl die Bundesregierung dessen Einsatz ursprünglich auch von §§ 100a ff., 161 StPO gedeckt sah[170].

1. § 100i I Nr. 1 StPO

Die Regelung beinhaltet die Möglichkeit der Strafverfolgungsbehörden, zur Vorbereitung einer Maßnahme nach § 100a StPO die Geräte- und die Kartennummer eines aktiv geschalteten Mobilfunkendgerätes zu bestimmen. Im Interesse der effektiven Strafverfolgung sei die Anordnung für eine zukünftige Telekommunikationsüberwachung unerlässlich. Für eine solche Überwachung sind u.a. auch die Karten- oder Gerätekennung (zumeist unbekannt[171]) nötig.
Durch diese Regelung wird eine Lücke geschlossen, da § 100g StPO nur die Anforderung von Verbindungsdaten „im Falle einer Verbindung“ (§ 100g III StPO) zulässt.

2. § 100i I Nr. 2 StPO

Weiterhin ist es nun möglich zur vorläufigen Festnahme oder zur Ergreifung eines Täters den Standort eines Mobilfunkgerätes im Stand-By-Betrieb zu bestimmen. Auch hier wird eine Ermittlungslücke zu § 100g StPO geschlossen.

3. Voraussetzungen, § 100i II 1, 2 StPO

a) Die **Bestimmung der Kennung** ist nur unter den Voraussetzungen des § 100a zulässig und auch nur, wenn eine sonstige Ermittlung nicht oder nur wesentlich erschwert möglich wäre (Subsidiarität).

---

[162] Näheres: Fox, DuD 2002, 4.
[163] Fox, DuD 2002, 4.
[164] BR-Drs. 369/1/97.
[165] „Der Spiegel“ 33/2001, S. 54f.; BT-Drs. 14/6827, S. 1, 2 vom 23.08.2001.
[166] 9. Januar 2002, BGBl. I, S. 361; Fox, DuD 2002, 212 (213).
[167] Fox, DuD 2002, 212 (213); ausführlich: Fox, IMSI-Catcher, DuD 1997, 539.
[168] Fox, DuD 2002, 212 (214).
[169] BGBl. I 2002, S. 3018; Hilger, GA 2002, 557 ff.
[170] BGBl. I 2002, S. 3018; vgl. BT-Drs 14/7562, mit Beschluss des 6. Ausschusses.
[171] BT-Drs. 14/9088, S. 7.

b) Die Ermittlung des Aufenthaltsortes (**Standortkennung**) ist nur im Falle einer Straftat von erheblicher Bedeutung zulässig, wenn die Ermittlung auf andere Weise weniger Erfolg versprechend oder erschwert wäre oder zur Eigensicherung der eingesetzten Polizeibeamten erforderlich ist.

4. Weitere Regelungen

Die Absätze 3 und 4 enthalten weitere Subsidiaritätsklauseln für die Erhebung personenbezogener Daten Dritter und die Anordnung der Maßnahmen durch den Richter unter Verweis auf die §§ 100a, b StPO.

Personenbezogene Daten von Dritten dürfen nur erhoben werden, wenn dies aus technischen Gründen zur Zweckerreichung unvermeidbar ist (Abs. 3, S. 1). Sind die Daten bereits erhoben, dürfen sie nicht über den Zweck der Ermittlung von Geräte- und Kartennummer hinaus verwertet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen (Abs. 3, S. 2).

Eine Anordnung darf grundsätzlich nur durch den Richter erfolgen (§ 100i IV 1 HS 1 i.V.m. § 100b I), in Vorbereitung einer Telefonüberwachung soll § 100b II 1 StPO entsprechend gelten (§ 100i IV 1 HS 2 StPO).

Eine Anordnung ist auf höchstens sechs Monate befristet, mit der Möglichkeit zur Verlängerung um weitere sechs Monate (§ 100i IV 2 StPO).

Letztendlich werden die Telekommunikationsunternehmen verpflichtet, bei der Standortermittlung gemäß Abs. 4, S. 3 u.a. den im Polizeidienst tätigen Hilfsbeamten der Staatsanwaltschaft die Geräte- und Kartennummer mitzuteilen.

5. Meinung

Eine Auseinandersetzung mit dem Thema, ob und in welchem Umfang der § 100i StPO hinsichtlich von Verbindungsdaten i.w.S. mit Grundrechten vereinbar, überhaupt verfassungsrechtlich korrekt zu Stande gekommen ist und welche Folgeprobleme sich in Abgrenzung zu Prävention und Repression ergeben, wäre in diesem Rahmen zu umfangreich und ist nicht Gegenstand dieser Arbeit zu den §§ 100g, h StPO.

Peter Eichhorn