Ergänzende Ausführungen zu Frage 37

Die deutsche Rechtslage erlaubt den Strafverfolgungsbehörden sowohl den Zugriff auf Bestandsdaten (Subscriber data), Verkehrsdaten (traffic data) als auch Inhaltsdaten (content data), wobei hierzu jeweils spezifische Anforderungen in den einschlägigen Befugnisnormen aufgestellt werden.

1.) Zugriff auf Bestandsdaten (subscriber data):

a) Bestandsdatenauskunft im Bereich des Telekommunikationsgesetzes:

Auf nach den §§ 95 und 111 Telekommunikationsgesetz (TKG) von den Diensteanbietern, die geschäftsmäßig Telekommunikationsdienste erbringen, gespeicherte Bestandsdaten (z.B. Daten bei Vertragsabschluss, Namen hinter E-Mail-Adressen oder Rufnummern, Rechnungsadressen, statische IP-Adressen; vgl. § 3 Nr. 3 TKG) kann nach der Regelung des § 100j Abs. 1 Satz 1 Strafprozessordnung (StPO) zugegriffen werden, wenn dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Ebenso darf nach § 100j Abs. 2 StPO eine entsprechende Auskunft zu den Bestandsdaten anhand einer (dynamischen) IP-Adresse verlangt werden. Eine besondere Anordnungskompetenz ist in diesen beiden Fallgestaltungen nicht vorgesehen, so dass die Anordnung sowohl durch die Staatsanwaltschaft als auch durch deren Ermittlungspersonen ergehen kann.

Soweit sich eine Bestandsdatenauskunft jedoch auf Daten bezieht, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, darf dies nur erfolgen, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen, wenn also die besonderen strafprozessualen Eingriffsbedingungen erfüllt sind. In den Fällen der Anforderung von Zugangssicherungscodes darf dies auf Antrag der Staatsanwaltschaft nur durch das Gericht angeordnet werden

(§ 100j Abs. 3 Satz 1 StPO). Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen ergehen (§ 100j Abs. 3 Satz 2 StPO), wobei die gerichtliche Entscheidung unverzüglich nachzuholen ist (§ 100j Abs. 3 Satz 3 StPO). Nur dann, wenn der Betroffene von einem entsprechenden (auf Zugangssicherungscodes bezogenen) Auskunftsverlangen bereits Kenntnis hat oder haben muss oder wenn die Nutzung der Daten bereits durch eine gerichtliche Entscheidung gestattet wird (z.B. im Rahmen eines Beschlagnahmebeschlusses), ist nach § 100j Abs. 3 Satz 4 StPO eine richterliche Anordnung entbehrlich.

b) Bestandsdatenauskunft im Bereich des Telemediengesetzes:

Auf von Telemediendienstanbietern (z.B. Ebay, YouTube, Facebook, Amazon u.a.) gespeicherte Bestandsdaten im Sinne des § 14 Abs. 1 Telemediengesetz (TMG) kann zugegriffen werden, wenn dies zur Strafverfolgung erforderlich ist (§ 14 Abs. 2 TMG). Unter Bestandsdaten im Sinne dieser Norm werden alle personenbezogenen Daten eines Nutzers verstanden, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen dem Diensteanbieter und dem Nutzer über die Nutzung von Telemedien erforderlich sind.

Der Zugriff auf diese Daten erfolgt durch die Strafverfolgungsbehörden auf Grundlage der allgemeinen strafprozessualen Eingriffsbefugnis der §§ 161 Abs.1, 163 Abs. 1 StPO, was zugleich bedeutet, dass es einer gerichtlichen Anordnung nicht bedarf.

2.) Zugriff auf Verkehrsdaten (traffic data):

Bezüglich des Begriffs der Verkehrsdaten darf zunächst darauf hingewiesen werden, dass angesichts der Ausführungen in Frage 34 und insbesondere in Frage 61 des Fragebogens, wonach der Zeitpunkt der Versendung einer E-Mail als "Meta data" bezeichnet wird, nachfolgend davon ausgegangen wird, dass dieser Begriff im Sinne der Verkehrsdaten, also der Daten, die den äußeren Rahmen der Nachricht umschreiben (wer hat wann mit wem zu welcher Zeit kommuniziert), verstanden wird.

Beim Zugriff auf im Bereich des Telekommunikationsverkehrs angefallene Verkehrsdaten (hierunter fallen nach § 3 Nr. 30 TKG alle Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden) ist maßgeblich danach zu unterscheiden, ob ein Zugriff auf solche Verkehrsdaten erfolgen soll, die von den Telekommunikationsdiensteanbietern für eigene Zwecke (insbesondere Abrechnungszwecke) nach § 96 TKG gespeichert wurden oder auf solche Daten, die im Rahmen der sog. Verkehrsdatenspeicherung im Sinne des § 113b TKG, also im Rahmen der Speicherpflicht, gespeichert wurden. Auf die Besonderheit der Funkzellendatenerhebung im Sinne des § 100g Abs. 3 StPO wird im Rahmen der nachfolgenden Ausführungen nicht eingegangen.

2.1) Zugriff auf zu eigenen Zwecken von den Diensteanbietern (gewissermaßen freiwillig) gespeicherte Verkehrsdaten:

Ein strafprozessualer Zugriff auf nach § 96 Abs. 1 TKG zu eigenen Zwecken (meist jedoch nur für einen begrenzten Zeitraum) gespeicherte Daten nach § 100g Abs. 1 Satz 1 StPO ist dann zulässig, wenn Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer

- eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 StPO bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat oder
- eine Straftat mittels Telekommunikation begangen hat

und die Verkehrsdatenerhebung für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Wenn eine Straftat mittels Telekommunikation begangen wurde, ist die Maßnahme gemäß § 100g Abs. 1 Satz 2 StPO nur zulässig ist, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre. Ein Zugriff auf nach § 96 Abs. 1 Nr. 1 TKG gespeicherte (also retrograde) Standortdaten ist nach der derzeit geltenden Regelung des § 100g Abs. 1 Satz 3 StPO (und nach Auslaufen der Überleitungsvorschrift des § 12 Abs. 1 EGStPO) ausgeschlossen.

Maßnahmen nach § 100g Abs. 1 StPO dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft (nicht durch ihre Ermittlungsperso-

nen!) getroffen werden. Die Eilanordnung der Staatsanwaltschaft tritt außer Kraft, wenn sie nicht binnen drei Werktagen vom Gericht bestätigt wird (§§ 101a Abs. 1 Satz 1 i.V.m. § 100e Abs. 1 Satz 1 bis 3 StPO).

b) Zugriff auf nach § 113b TKG gespeicherte Verkehrsdaten:

Der Zugriff auf von den Telekommunikationsdiensteanbietern auf Grundlage der in § 113b TKG gesetzlich vorgesehenen (derzeit aufgrund einer Entscheidung des Oberverwaltungsgerichts Münster vom 22.06.2017 und einer Mitteilung der Bundesnetzagentur vom 28.06.2017 aber faktisch ausgesetzten) Speicherpflicht vorgehaltene Verkehrsdaten darf hingegen nur in den engen Voraussetzungen des § 100g Abs. 2 StPO erfolgen. Ausdrücklich hingewiesen werden muss auf den Umstand, dass - im Gegensatz zu der bis zum 02.03.2010 geltenden Rechtslage - die Anbieter von elektronischer Post bzw. E-Mail-Diensten gerade nicht zu den Speicherverpflichteten i.S.v. § 113b TKG (eingeführt mit Gesetz vom 10.12.2015 (BGBl. 2015 I 2218 ff.) gehören.

Der Zugriff auf diese Daten ist - soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht - nur dann statthaft, wenn

- jemand als Täter oder Teilnehmer eine der in Satz 2 bezeichneten besonders schweren Straftaten begangen hat oder in Fällen, in denen der Versuch strafbar ist, eine solche Straftat zu begehen versucht hat und
- die Tat auch im Einzelfall besonders schwer wiegt.

Während beim Zugriff auf nach § 96 TKG gespeicherte Verkehrsdaten also eine Straftat von im Einzelfall erheblicher Bedeutung, insbesondere eine (schwere) Straftat im Sinne des Straftatenkatalogs des § 100a Abs. 2 StPO genügt, setzt ein Zugriff auf nach § 113b TKG gespeicherte Verkehrsdaten eine "besonders schwere Straftat" im Sinne des - gegenüber § 100a Abs. 2 StPO deutlich engeren - Straftatenkatalogs des § 100g Abs. 2 Satz 2 StPO voraus.

Auch für eine Verkehrsdatenerhebung auf Grundlage des § 100g Abs. 2 StPO bedarf es - wie oben bereits zur Verkehrsdatenerhebung nach § 100g Abs. 1 StPO ausgeführt - auf Grundlage des §§ 101a Abs. 1 Satz 1 i.V.m. § 100e Abs. 1 Satz 1 StPO einer gerichtlichen Anordnung. Anders als dort ist jedoch bei einer Verkehrsdatenerhebung nach § 100g Abs. 2 StPO ein Eilkompetenz der Staatsanwaltschaft bei Gefahr im Verzug ausgeschlossen. Es gilt also ein ausschließlicher Richtervorbehalt (vgl. § 101a Abs. 1 Satz 2 StPO).

3.) Zugriff auf Inhaltsdaten (content data):

3.1) Der verdeckte Zugriff auf Inhaltsdaten kann, soweit ein Telekommunikationsvorgang nicht abgeschlossen ist, ausschließlich auf Grundlage des § 100a StPO im Rahmen einer Telekommunikationsüberwachungsmaßnahme erfolgen.

Eine entsprechende Anordnung setzt voraus, dass

- bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100a Absatz 2 StPO (abschließend) bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,
- die Tat auch im Einzelfall schwer wiegt und
- die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Eine solche Telekommunikationsüberwachungsmaßnahme darf auf Antrag der Staatsanwaltschaft nur durch das Gericht angeordnet werden (§ 100e Abs. 1 Satz 1 StPO). Jedoch kann gemäß § 100e Abs. 1 Satz 2 StPO bei Gefahr im Verzug (also in Eilfällen) die Anordnung durch die Staatsanwaltschaft (nicht durch deren Ermittlungspersonen) getroffen werden. Sie tritt, wenn sie nicht binnen drei Werktagen vom Gericht bestätigt wird, gemäß § 100e Abs. 1 Satz 3 StPO außer Kraft. Darüber hinaus ist die Maßnahme auf höchstens drei Monate zu befristen, wobei eine Verlängerung um jeweils nicht mehr als drei Monate zulässig ist, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen (§ 100e Abs. 1 Satz 4 und 5 StPO). Die Einzelheiten betreffend die Ausleitung der Erkenntnisse an die Strafverfolgungsbehörden oder

auch die Übermittlung der Anordnungen an die Verpflichteten regelt das Telekommunikationsgesetz (TKG) und die Telekommunikationsüberwachungsverordnung (TKÜV).

3.2) Auch wenn ein Telekommunikationsvorgang abgeschlossen ist, ist ein Zugriff auf Inhaltsdaten möglich.

a) Zugriff auf E-Mails beim Provider

Soweit nach abgeschlossenem Telekommunikationsvorgang ein Zugriff auf beim Mail-Provider zwischen- oder endgespeicherte Daten erfolgen soll, ist danach zu unterscheiden, ob der Zugriff offen oder verdeckt erfolgen soll.

Hierzu wurden in der Rechtsprechung und Literatur zunächst unterschiedliche Ansätze vertreten. Seit der Entscheidung des Bundesverfassungsgerichts vom 16.06.2009 (NJW 2009, 2431) ist hinreichend geklärt, dass die §§ 94 ff. StPO eine hinreichende Rechtsgrundlage zur Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers darstellen, wobei jedoch zu beachten ist, dass die §§ 94 ff. StPO als "offene Maßnahmen" ausgestaltet sind, also dem davon Betroffenen und den Verfahrensbeteiligten bekannt zu machen sind (§§ 33 Abs. 1, 35 Abs. 2 StPO).

Das Bundesverfassungsgericht hat in der genannten Entscheidung aber auch deutlich gemacht, dass bei einem verdeckten Zugriff §§ 94, 98 StPO als Eingriffsgrundlage ausscheiden, da hier besonders hohe Anforderungen an die Bedeutung der zu verfolgenden Straftat und den für den Zugriff erforderlichen Grad des Tatverdachts zu stellen sind. Während vor diesem Hintergrund ein Teil der Literatur und Rechtsprechung nunmehr ausschließlich eine Anordnung auf § 100a StPO stützen will, lässt eine andere Auffassung auch eine Postbeschlagnahme im Sinne von § 99 StPO genügen (vgl. hierzu Graf in Beck`scher Online-Kommentar StPO, 27. Edition (Stand: 01.01.2017) § 100a StPO Rn. 26 ff. m.w.N.).

Zu den Anordnungsvoraussetzungen bei Annahme des § 100a StPO kann auf die obigen Ausführungen verwiesen werden. Geht man mit der hiesigen Praxis hingegen von der Einschlägigkeit des § 99 StPO aus, dann gilt es § 100 StPO zu beachten. Dieser bestimmt in Abs. 1, dass die Beschlagnahme ebenfalls einer Anordnung des Gerichts bedarf und bei Gefahr im Verzug durch die Staatsanwalt-

schaft (nicht auch von Ermittlungspersonen der Staatsanwaltschaft!) angeordnet werden darf, welche außer Kraft tritt, wenn sie nicht binnen drei Werktagen vom Gericht bestätigt wird (§ 100 Abs. 2 StPO). Darüber hinaus kann bei einer Maßnahme gemäß § 99 StPO nach dem Wortlaut des § 100 Abs. 3 StPO die Durchsicht des Postfachinhalts nur auf die Staatsanwaltschaft (nicht auf die Ermittlungspersonen) übertragen werden.

b) Zugriff auf Daten beim Beschuldigten:

Ein Zugriff auf im Rechner des Beschuldigten (oder Dritten) abgespeicherten E-Mails ist (unter Berücksichtigung der oben genannten Entscheidung des Bundesverfassungsgerichts) auf Grundlage der §§ 94 ff. StPO möglich, soweit es sich um eine **offene** Ermittlungsmaßnahme (also Durchsuchung und Beschlagnahme) handelt.

Bei Durchsuchungsmaßnahmen ist auch zu berücksichtigen, dass § 110 Abs. 3 Satz 1 StPO es bei Durchsicht von elektronischen Speichermedien auch gestattet, auf hiervon räumlich getrennte Speichermedien, soweit auf sie von dem Speichermedium aus zugegriffen werden kann, erstreckt werden kann, wenn anderenfalls der Verlust der gesuchten Daten zu besorgen ist. Satz 2 dieser Regelung gestattet es auch, Daten, die für die Untersuchung von Bedeutung sein können, zu sichern.

c) Online-Durchsuchung eines informationstechnischen Systems

Am 24.08.2017 ist das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens in Kraft getreten ist (vgl. BGBl. 2017 I S. 3202 ff.). Dieses beinhaltet mit einem neuen § 100b StPO nun erstmals eine strafprozessuale Eingriffsbefugnis für den verdeckten Zugriff auf informationstechnische Systeme (sog. Online-Durchsuchung).

Eine derartige Maßnahme darf ergriffen werden, wenn

- bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Abs. 2 bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat,
- die Tat auch im Einzelfall besonders schwer wiegt und
- die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Grundsätzlich darf sich eine entsprechende Maßnahme nur gegen den Beschuldigten richten. Ein Eingriff in informationstechnische Systeme Dritter ist nur beim Vorliegen der - kumulativ zu erfüllenden - Voraussetzungen des § 100b Abs. 3 Satz 2 Nr. 1 und 2 StPO zulässig.

Der Katalog der "besonders schweren Straftaten" ist insoweit deutlich enger gefasst als der Katalog der "schweren Straftaten" im Sinne von § 100a Abs. 2 StPO.

Aufgrund der besonderen Eingriffsintensität dieser Maßnahme wurden hier weitgehend die zuvor nur für die Akustische Wohnraumüberwachung geltenden strengen Verfahrensvorschriften auf die "Online-Durchsuchung" erstreckt. So darf die Maßnahme auf Antrag der Staatsanwaltschaft nur durch eine in § 74a Abs. 4 Gerichtsverfassungsgesetz (GVG) genannte Strafkammer des Landgerichts angeordnet werden (§ 100e Abs. 2 Satz 1 StPO). Eine Entscheidung des Ermittlungsrichters genügt somit nicht. Bei Gefahr im Verzug ist auch eine Anordnung durch die Staatsanwaltschaft ausgeschlossen. In Eilfällen ist nach § 100e Abs. 2 Satz 2 StPO nur eine Anordnung des Kammervorsitzenden genügend. Diese tritt außer

Kraft, wenn die Strafkammer diese Anordnung nicht binnen drei Werktagen bestätigt (§ 100e Abs. 2 Satz 3 StPO). Darüber hinaus kann die Maßnahme auch nur auf ein Monat befristet werden und kann in der Folge jeweils nur um einen Monat verlängert werden, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Wenn die Maßnahme auf insgesamt sechs Monate verlängert werden muss, entscheidet über weitere Verlängerungen ein Strafsenat des Oberlandesgerichts (vgl. § 100e Abs. 2 Satz 4-6 StPO).

3.3) Zugriff auf Nutzungsdaten im Sinne des Telemediengesetzes:

Unter Nutzungsdaten werden im Anwendungsbereich des TMG insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien verstanden (§ 15 Abs. 1 Satz 2 TMG).

Für Nutzungsdaten im Sinne des Telemediengesetzes sieht § 15 TMG eine eigenständige Regelung dafür vor, dass derartige Daten von den Telemediendiensteanbietern gespeichert werden dürfen. Indem § 15 Abs. 4 Satz 4 TMG auf § 14 Abs. 2 bis 5 TMG verweist, dürfen auch diese Daten (u.a.) an die Strafverfolgungsbehörden weitergegeben werden, wenn dies für Zwecke der Strafverfolgung erforderlich ist. Wie oben bereits zu den Bestandsdaten ausgeführt, erfolgt der Zugriff auf diese Daten auf Grundlage der allgemeinen strafprozessualen Eingriffsbefugnis der §§ 161 Abs.1, 163 Abs. 1 StPO, was zugleich bedeutet, dass es dem Grundsatz nach einer gerichtlichen Anordnung nicht bedarf. In der Praxis verlangen die Telemediendiensteanbieter bei Nutzungsdaten jedoch meist zumindest eine staatsanwaltschaftliche Anfrage gem. §§ 161, 163 StPO. In Einzelfällen wird sogar ein Durchsuchungs- und Beschlagnahmebeschluss gem. §§ 94, 98, 103 StPO gefordert.