JUCONOMY
RECHTSANWÄLTE

TK-Überwachung

Universität Münster

Vorlesung
RA Dr. Peter Schmitz

Münster, 03. Dezember 2010

JUCONOMY Rechtsanwälte
Düsseldorf

Inhaltsübersicht

Grundzüge der Telekommunikationsüberwachung

- Systematik der TKÜ anhand der StPO
- Neuregelung ab dem 01.01.2008 – Übersicht
- Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Grundzüge der Telekommunikationsüberwachung

- TK-Überwachung im engeren Sinn
  - Inhalt und „nähere Umstände“ (Verkehrsdaten)
  - §§ 100a, 100b StPO, G 10-G, ZFdG, LPolG
- TK-Überwachung im weiteren Sinn
  - Auskunft über Bestandsdaten (§ 113 TKG)
  - Auskunft über Verkehrsdaten (§§ 100g, 100h StPO, BVerfSchg, LVerfSchg, BND-G, MAD-G)
  - Einsatz eines IMSI-Catchers (§ 100i StPO)

Übersicht - Telekommunikationsüberwachung

- Auskunft über Bestandsdaten (§§ 111 - 113 TKG)
  - Gegenstand: Bestandsdaten / „Identifizierungsdaten“ im Sinne des § 111 TKG
  - Verpflichteter: geschäftsmäßiger Erbringer von Telekommunikationsdiensten
  - Auskunftsberechtigt: Behörden i. S. d. § 113 Abs. 1 TKG
  - Anordnung: Behörden i. S. d. §113 Abs. 1 TKG / nicht: „Private“

- Auskunft über Verkehrsdaten (§100g, 100h StPO)
  - Gegenstand: Verkehrsdaten
  - Verpflichteter: (geschäftsmäßiger) Erbringer von Telekommunikationsdiensten
  - Auskunftsberechtigt: Strafverfolgungsbehörden / nicht: „Private“
  - Anordnung: grds. Richter / StA bei Gefahr im Verzug

- Überwachung der Telekommunikation (§100a, 100b StPO)
  - Gegenstand: Inhalt der TK und Verkehrsdaten
  - Verpflichteter: (geschäftsmäßiger Erbringer) von Telekommunikationsdiensten
  - Auskunftsberichtigt: Strafverfolgungsbehörden / nicht: „Private“
  - Anordnung: grds. Richter / StA bei Gefahr im Verzug

Übersicht – Weitere Ermittlungsmöglichkeiten der Strafverfolgungsbehörden

- Durchsuchung (§§ 102 ff StPO)
  - Gegenstand: Räumlichkeiten und Gegenstände
  - Anordnung: Richter / StA und Polizei bei Gefahr im Verzug

- Beschlagnahme (§§ 94, 98 StPO)
  - Gegenstand: Gegenstände (Ausnahme: § 97 StPO)
  - Anordnung: Richter / StA und Polizei bei Gefahr im Verzug

- Herausgabeverlangen (§ 95 StPO)
  - Gegenstand: im Einzelfall konkretisierte Beweismittel
  - Anordnung: Richter / StA

- Zeugenvernehmung (§§ 161a, 163a StPO)
  - Gegenstand: beliebig
  - Anordnung
    - bindend: Richter / StA
    - freiwillig: Polizei

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
  - **Systematik der TKÜ anhand der StPO**
    - **Auskunft über Bestandsdaten (§ 113 TKG)**
  - Neuregelung ab dem 01.01.2008 – Übersicht
  - Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Auskunft über Bestandsdaten im manuellen Auskunftsverfahren: § 113 TKG

- Gegenstand der Auskunft - Bezugnahme auf §§ 95 und 111 TKG
  - Bestandsdaten (§ 95 TKG)
    - Informationen zur inhaltlichen Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über TK-Dienste (§ 3 Nr. 3 TKG)
    - Vorratsdatenspeicherung nur im Fall des § 111 TKG
  - nicht: Daten, die dem Fernmeldegeheimnis unterstehen (§ 113 Abs. 1 TKG)
  - Problem: **dynamische IP-Adresse** – 3 Argumentationsansätze (vereinfacht):
    - Verbindungszeitpunkt bereits bekannt → Bestandsdatum wird mitgeteilt
    - Auswertung von Verkehrsdaten erforderlich und Bezug zu Telekommunikation → Verkehrsdatum
    - Rspr. uneinheitlich; **Tendenz** zu Bestandsdatum, anders aber z.B. § 101 UrhG
    - **BVerfG**: Mittelweg: Eingriff in Fernmeldegeheimnis (also Verkehrsdaten betroffen), aber geringere Anforderungen an Auskunftserteilung, da den Sicherheitsbehörden am Ende nur die „Bestandsdaten“ bekannt werden. Allerdings ist gesetzliche Regelung zur Auskunftserteilung an den Betroffenen erforderlich.
  - „Zugriffsinformationen“ (**PIN / PUK**): § 113 Abs. 1 S. 2 TKG --> nach §§ 161 Abs. 1, 163 Abs. 1 StPO
    → *aber* verfassungsrechtlich bedenklich, weil Zugriff auf Telekommunikation möglich
    - keine Verpflichtung zum Entschlüsseln eines verschlüsselt gespeicherten Passworts
    - keine Verpflichtung zum Zurücksetzen, falls Passwort/PIN nicht bekannt

Auskunft über Bestandsdaten manuelles Auskunftsverfahren: § 113 TKG

- Auskunftspflichtige: „geschäftsmäßige Erbringer von Telekommunikationsdiensten“ (§ 3 Nr. 10 TKG)
  - nachhaltiges Angebot von Telekommunikation
  - nicht erforderlich: Gewinnerzielungsabsicht
  - unbeachtlich: geschlossene Benutzergruppe (*arg e* § 91 Abs. 2 TKG)

- Ziel des Auskunftsverlangens
  - „Verfolgung von Straftaten, Ordnungswidrigkeiten und zur Gefahrenabwehr“
  - nicht: privatrechtliche Interessen

Auskunft über Bestandsdaten: § 113 TKG (manuelles Verfahren)

- Auskunftserteilung
  - **Unverzüglichkeit**
    - § 113 Abs. 2 TKG Pflicht zu „erforderlichen Vorkehrungen“ (auf eigene Kosten) – weitgehend unklar aus rechtlicher Sicht → Personal und Technik?
    - als Vorbild?: BNetzA selbst schränkt Auskunftsbereitschaft im Rahmen von § 112 TKG ein
  - im Einzelfall
    - direkte Anfrage der Sicherheitsbehörden
    - **≠ automatisiertes Auskunftsverfahren (§ 112 TKG)**
      - Datenbank
      - Abfrage durch BNetzA, nicht aber Sicherheitsbehörden
  - Entschädigung (§ 113 Abs. 2 TKG a. E.)
  - **Verschwiegenheitspflicht** (§ 113 Abs. 1 TKG a. E.)
- Sanktion
  - Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig: Bußgeld
  - Auskunft über PIN/PUK/Passwort an andere als dort genannte Stelle: Bußgeld
  - Verstoß gegen Verschwiegenheit: Bußgeld

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
  - **Systematik der TKÜ anhand der StPO**
    - **Auskunft über Verkehrsdaten (§§ 100g, 100h StPO)**
  - Neuregelung ab dem 01.01.2008 – Übersicht
  - Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Auskunft über Verkehrsdaten (§§ 100g, 100h StPO)

- Gegenstand der Auskunft: „Telekommunikationsverbindungsdaten“
  - Definition in § 100g Abs. 3 StPO
    - **Vergangenheit**: datenschutzkonform (noch) gespeicherte
    - **Zukunft**: datenschutzkonform aus Eigeninteresse (str.) erhobene
    - Inverse-Auskunft (§ 100g Abs. 2 StPO)
  - (formal) nicht: TMG-Nutzungsdaten
  - Problem: dynamische IP-Adresse (siehe § 113 TKG)
- Auskunftserteilung: unverzüglich
- Auskunftspflichtige: „geschäftsmäßige Erbringer von Telekommunikationsdiensten“ (§ 3 Nr. 10 TKG)
- **Grund des Auskunftsverlangens**: „Straftat von erheblicher Bedeutung“ oder „mittels einer Endeinrichtung (§ 3 Nr. 3 TKG) begangen“ (bezieht sich auf TKG a. F.)
- **Anordnung** (§ 100g Abs. 2 i. V. m. § 100b Abs. 1 StPO)
  - **grds. richterliche Anordnung**: max. 3 Monate
  - Eilanordnung der StA: max. 3 Tage
  - keine Anordnung durch Polizei
- Exkurs: § 8 Abs. 8 BVerfSchG, LVerfSchG, § 8 Abs. 3a BNDG, § 10 Abs. 3 MADG

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
  - **Systematik der TKÜ anhand der StPO**
    - **Überwachung der Telekommunikation (§§ 100a, 100b StPO)**
  - Neuregelung ab dem 01.01.2008 – Übersicht
  - Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Übersicht: §§ 100a, 100b StPO

- Gegenstand: „Telekommunikation“
  - „Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen“(§ 100b Abs. 3 S. 1 StPO) (keine Begrenzung durch TKÜV)
  - **Inhalt**
  - **„nähere Umstände“** / Verkehrsdaten
- Verpflichteter: „geschäftsmäßige Erbringer von Telekommunikationsdiensten“ (§ 3 Nr. 10 TKG)
- berechtigt: Strafverfolgungsbehörden / keine Anordnung durch Polizei
- Grund: Straftat aus dem Katalog des § 100a S. 1 StPO
- **Anordnung** (§ 100b Abs. 1 StPO)
  - **grds. richterliche Anordnung**: max. 3 Monate
  - Eilanordnung der StA: max. 3 Tage
- Exkurs: §§ 3, 5, 8 G 10-G, §§ 23a – 23c, 23e ZFdG, Polizei- bzw. Ordnungs- bzw. Sicherheitsgesetze der Länder

Pflichten - §§ 100a, 100b StPO

- Exkurs: TKÜV (§ 110 TKG)
  - gilt für „Vorkehrung“ zum Ermöglichen der Überwachung und Aufzeichnung, wenn mehr als 10.000 Anschlüsse
  - Kreis der Verpflichteten nicht zwingend gleich §§ 100a, 100b StPO
    - Begrenzung durch § 110 TKG auf: Telekommunikationsdienste für die Öffentlichkeit
    - weitere Begrenzungen durch TKÜV
  - § 5 Abs. 2 TKÜV: Bereitstellung einer vollständigen Kopie der Telekommunikation
  - § 6 TKÜV: unverzügliche Umsetzung einer Anordnung
  - § 12 TKÜV: Vorhaltung personeller Ressourcen zur Umsetzung und Entgegennahme von Anordnungen

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
  - Systematik der TKÜ anhand der StPO
  - **Neuregelung ab dem 01.01.2008 – Übersicht**
  - Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Ausweitung der Pflichten zur TK-Überwachung in der StPO

- **Erweiterung des Kreises der Verpflichteten** durch § 100b Abs. 3 StPO n. F. für:
  - TK-Überwachung (Inhalt & Verkehrdaten) im konkreten Einzelfall
  - Auskunftserteilung über Verkehrsdaten im konkreten Einzelfall
  - ≠ Pflicht zu standardisierten techn. „Vorab-Maßnahmen“
- **bisher**: „geschäftsmäßige Erbringen von TK-Diensten“ i. S. v. § 3 Nr. TKG
  - TK durch Konzernunternehmen bzw. Gestattung der Privatnutzung
- **zukünftig in StPO**: Erbringen von „TK-Diensten“ i. S. v. § 3 Nr. 24 TKG
  - Intention des Gesetzgebers - Ausweitung auf
    - TK im Unternehmen
    - „geschlossene Benutzergruppen“
  - gelungen?: Wortlaut <-> praktische Handhabung
- **Abgrenzung von**: Pflicht zu standardisierten „Vorab-Maßnahmen“ (TKG/TKÜV)
  - Einschränkung durch TKG: TK-Dienst für die Öffentlichkeit
    - **„altes“ TKG**: (-) bei geschlossener Benutzergruppe
    - **„Rein-/Raus-TK“** bei geschlossener Benutzergruppe?
    - Nutzbarkeit für **„jedermann“**?
  - **Einschränkung durch TKÜV**: > 10.000 Teilnehmeranschlüsse

Veränderung der Befugnisse und Pflichten nach der StPO

- TK-Überwachung (§ 100a StPO) und Auskunftspflicht (§ 100g StPO)
  - **bisher**: Mitwirkungspflicht der Verpflichteten
  - **neu**: eigenständige Erhebungsbefugnis der Strafverfolger
  - ➔ Eingriffe in die „Netzhoheit“ der TK-Unternehmen
- Auskunftspflicht über Verkehrsdaten:
  - **neuer Gegenstand**: Verkehrsdaten im Sinne von §§ 96 Abs. 1, (aufgehoben *113a TKG)* (**bisher**: TK-Verbindungsdaten explizit festgelegt in § 100g Abs. 3 StPO)
  - **neu**: Echtzeitausleitung der Verkehrsdaten bei zukunftsbezogener Auskunft über Verkehrsdaten nach § 100g StPO n. F.
  - technische Ausgestaltung der **Echtzeitausleitung**
    - durch TKÜV
    - Beschränkung standardisierter techn. „Vorab-Maßnahmen“ auf TK-Dienste für die Öffentlichkeit
    - bisher nicht geklärt

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
  - Systematik der TKÜ anhand der StPO
  - Neuregelung ab dem 01.01.2008 – Übersicht
  - **Abgrenzung der Spezialermächtigungen von Durchsuchung, Beschlagnahme, Herausgabeverlangen und Zeugenvernehmung**
- Vorratsdatenspeicherung
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Abgrenzung zu den Spezialermächtigungen: Fernmeldegeheimnis

- BVerfG, Urt. v. 4.2.2005 (2 BvR 308/04) – Auslesen einer SIM-Karte: Beschlagnahme eines Mobiltelefons und Auslesen der Daten
  - unzulässige Umgehung des Art. 10 GG, wenn das Nichtvorliegen der Voraussetzungen von §§ 100g, 100h StPO durch Rückgriff auf Maßnahme mit geringeren Anforderungen umgangen würde

    „Die auf Art. 10 Abs. 2 GG beruhende Begrenzungsfunktion der §§ 100g und 100h verbietet den Ermittlungsbehörden die Umgehung der dort geregelten materiellen und verfahrensmäßigen Beschränkungen durch die Wahl einer anderen Zwangsmaßnahme, die solchen Schranken nicht unterliegt.“

  - Fazit: Information muss entsprechend der Spezialermächtigung beschafft werden

Abgrenzung zu den Spezialermächtigungen: Fernmeldegeheimnis

- BVerfG, Urt. v. 2.3.2006 (2 BvR 2099/04) – Beschlagnahme von E-Mails
  - **dreistufiges Verhältnis mit Blick auf Eingriffsbefugnisse**
    - Fernmeldegeheimnis (Art. 10 GG): Spezialermächtigung
    - Informationelle Selbstbestimmung (Art. 2 i.V.m. Art. 1 GG) mit besonderem Bezug zum Fernmeldegeheimnis: Beschlagnahme mit besonderen Anforderungen an die Verhältnismäßigkeit
    - Informationelle Selbstbestimmung (Art. 2 i.V.m. Art. 1 GG): „normale“ Beschlagnahme
  - **Reichweite des Schutzbereichs** präzisiert
    - **Abschluss des Übertragungsvorgangs**

      „*Wird der laufende Kommunikationsvorgang überwacht, liegt ein Eingriff in das Fernmeldegeheimnis auch dann vor, wenn die Erfassung des Nachrichteninhalts am Endgerät erfolgt. Die Einheitlichkeit des Übermittlungsvorgangs steht hier einer rein technisch definierten Abgrenzung entgegen (vgl. BVerfGE 106, 28, <38>).*“
    - **Beherrschbarkeit durch den Kommunikationsteilnehmer**

      „*Art. 10 Abs. 1 GG soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und will den Gefahren begegnen, die sich aus dem Übermittlungsvorgang einschließlich der Einschaltung eines Dritten ergeben (vgl. BVerfGE 85, 386 <396>; 106, 28 <36>; 107, 299 <313>).*“

Abgrenzung zu den Spezialermächtigungen: Fernmeldegeheimnis

- BVerfG, Beschl. v. 29.06.2006 (2 BvR 902/06) – Beschlagnahme von E-Mails
  - Eilrechtsschutz; nur kursorische Abwägungsentscheidung
  - Eilrechtsschutz für den Fall des Zugriffs bei einem Provider ohne Anwendung des Spezialermächtigungen
  - rechtliche Klärung steht noch aus
- Bedeutung für Provider: Schutz endet nicht für Daten in ihrem Herrschaftsbereich?
  - alleinige Beherrschbarkeit durch TK-Teilnehmer (-)
  - außerhalb der Sphäre des Teilnehmer besteht Gefahrlage in Form des Zugriffs bei einem Dritten
- Reaktion auf Umgehungsversuche durch Zeugenvernehmung, Durchsuchung und Beschlagnahme
  - vorbereitete schriftliche Stellungnahme mit Bezug auf Art. 10 GG
  - Auskunftsverweigerung

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
- **Vorratsdatenspeicherung**
- Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung

Was bedeutet Vorratsdatenspeicherung?

- Speicherung für im Zeitpunkt der Speicherung noch unbestimmte Zwecke
  - **unabhängig von der Erforderlichkeit** (z. B. Vertragsabschluss und Abrechnung)
  - **alleiniger Zweck: Auskunftserteilung** an
    - Sicherheitsbehörden (§§ 111 ff., 113a Abs. 10 TKG n. F.)
    - auch?: Private (z. B. Urheberrechtsinhaber)
- **bereits 2004** eingeführt: Vorratsdatenspeicherung für die in § 111 TKG festgelegten **„Identifizierungsdaten“** (Überschneidung zu „Bestandsdaten“)
  - Erhebungs- und Speicherpflicht „auf Vorrat“
  - Auskunft nach §§ 112, 113 TKG
  - neu: Erweiterung zum 01.01.2008 erfolgt auf
    - „Anschlusskennung“ / „Gerätekennung“
    - E-Mail-Dienste, insbes. Web-Mail-Dienste
- **neu:** Vorratsdatenspeicherung in § 113a TKG n. F. genannter **Verkehrsdaten**
  - keine Erhebungspflicht, nur Speicherpflicht

- **Inhalt der *aufgehobenen* Pflicht zur Vorratsdatenspeicherung**
  - Gegenstand: Verkehrsdaten i. S. d. §§ 96, 113a Abs. 2 bis 5 TKG n. F.
  - **keine Erhebungspflicht**; d. h. Daten müssen zwei Voraussetzungen kumulativ erfüllen:
    - im Rahmen des betrieblichen Eigeninteresses des Verpflichteten als Verkehrsdaten erhoben
    - im Katalog des § 113a Abs. 2 bis 5 TKG n. F. genannt
  - Speicherdauer
    - § 113 Abs. 1 S. 1 TKG n. F.: **6 Monate**
    - § 113 Abs. 11 TKG n. F.: Löschung innerhalb von 1 Monat nach Ablauf der Frist in § 113a Abs. 1 TKG n. F.

      → d. h. keine taggenaue Löschung erforderlich, **monatliche Löschroutine ausreichend**
  - keine Speicherung von Inhalten (§ 113a Abs. 10 TKG)
    - „Inhalt der Kommunikation“ (Problem bspw.: SMS)
    - Ziel-IP-Adresse ist nicht in Katalog des § 113a Abs. 4

- **Verfassungswidrigkeit der §§ 113a, 113b TKG a. F.**

- BVerfG, Urt. v. 02.03. 2010 (1 BvR 256/08, 1 BvR 263/08 , 1 BvR 586/08)
  - Speicherung von Verkehrsdaten auf Vorrat ist nicht per se grundrechtswidrig
  - Ausgestaltung einer solchen Vorratsdatenspeicherung in Form der §§ 113a, 113b TKG genügt nicht von Art. 10 Abs. 1 GG
- **Konsequenz der Verfassungswidrigkeit der §§ 113a, 113b TKG a. F.**
  - Löschung der „auf Vorrat“ nach §§ 113a, 113b TKG gespeicherten Daten
  - Keine Auskunft über solche Verkehrsdaten an Strafverfolgungsbehörden
  - Fortgelten der Auskunftspflicht in Bezug auf §§ 96, 97 TKG

- **Dreh- und Angelpunkt der Zulässigkeit**
  - dezentrale Speicherung bei den Telekommunikationsunternehmen
  - anstatt Speicherung bei staatlichen Einrichtungen
- **Gewährleistung eines besonders hohen Standards der Datensicherheit**
  mehr als nach § § 9 BDSG, 109 TKG
  Dynamisch nach dem Stand der Technik
  „Horrorkabinett“ für Telekommunikationsunternehmen
- **Ausgestaltung der Auskunftsregelung mitentscheidend für Verfassungsmäßigkeit**
  - Verhältnismäßig hohe Anforderungen
  - Transparenz – jedenfalls durch nachträgl. Benachrichtig.
  - Rechtsschutz

Vorratsdatenspeicherung nicht *per se* verfassungswidrig

BVerfG, Urt. v. 02.03. 2010 (1 BvR 256/08, 1 BvR 263/08 , 1 BvR 586/08) – Leitsätze 1 - 5

*„1. Eine sechsmonatige, **vorsorglich anlasslose Speicherung** von Telekommunikationsverkehrsdaten **durch private Diensteanbieter**, wie sie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 (ABl L 105 vom 13. April 2006, S. 54; im Folgenden: Richtlinie 2006/24/EG) vorsieht, ist mit Art. 10 GG **nicht schlechthin unvereinbar**; auf einen etwaigen Vorrang dieser Richtlinie kommt es daher nicht an.*

*2. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die gesetzliche Ausgestaltung einer solchen Datenspeicherung dem besonderen Gewicht des mit der Speicherung verbundenen Grundrechtseingriffs angemessen Rechnung trägt. Erforderlich sind **hinreichend anspruchsvolle und normenklare Regelungen** hinsichtlich der **Datensicherheit**, der **Datenverwendung**, der **Transparenz** und des **Rechtsschutzes**.*

3. *Die **Gewährleistung der Datensicherheit** sowie die normenklare **Begrenzung der Zwecke der möglichen Datenverwendung** obliegen als untrennbare Bestandteile der Anordnung der Speicherungs-verpflichtung **dem Bundesgesetzgeber** gemäß Art. 73 Abs. 1 Nr. 7 GG. Demgegenüber richtet sich die Zuständigkeit für die Schaffung der Abrufregelungen selbst sowie für die **Ausgestaltung der Transparenz- und Rechtsschutzbestimmungen** nach den jeweiligen Sachkompetenzen.*

4. *Hinsichtlich der **Datensicherheit** bedarf es Regelungen, die einen besonders **hohen Sicherheitsstandard normenklar und verbindlich** vorgeben. Es ist jedenfalls dem Grunde nach gesetzlich sicherzustellen, dass sich dieser **an dem Entwicklungsstand der Fachdiskussion** orientiert, neue Erkenntnisse und Einsichten **fortlaufend aufnimmt** und **nicht unter dem Vorbehalt einer freien Abwägung mit allgemeinen wirtschaftlichen Gesichtspunkten steht**.*

5. *Der **Abruf und die unmittelbare Nutzung der Daten** sind nur verhältnismäßig, wenn sie **überragend wichtigen Aufgaben des Rechtsgüterschutzes** dienen. Im Bereich der **Strafverfolgung** setzt dies einen **durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat** voraus. Für die **Gefahrenabwehr und die Erfüllung der Aufgaben der Nachrichtendienste** dürfen sie nur bei Vorliegen **tatsächlicher Anhaltspunkte für eine konkrete Gefahr für** Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für eine gemeine Gefahr zugelassen werden.*“

Inhaltsübersicht

- Grundzüge der Telekommunikationsüberwachung
- Vorratsdatenspeicherung
- **Exkurs: Durchsuchung externer Speichermedien und Abgrenzung zur Telekommunikationsüberwachung**

- **Durchsuchung externer Speichermedien, § 110 Abs. 3 StPO**
  - **Ziel:** „offene Online-Durchsuchung“ (Begründung S. 70)
  - Erstreckung der Durchsicht nach § 110 StPO auf:
    - **„räumlich getrennte Speichermedien“**
    - Konstellation: Durchsuchung einer Wohnung; Feststellung der Nutzung andernorts vorgehaltener Speichermedien → Zugriff externen Speicher
  - Grenze?: Entscheidungsbefugnis des Betroffenen, Dritten Zugang zu den andernorts gespeichert Daten zu ermöglichen
    - Regierungs-Entwurf: „*… auf die der Betroffene den Zugriff zu gewähren berechtigt ist, …*“
    - bspw. nicht bei Telearbeitsplätzen bzgl. Zugang zu Systemen des Arbeitgebers (so Gesetzesbegründung)
    - kein Ausschluss der zwangsweisen Durchsetzung
  - ➔ Sicherheitsrisiko durch unbemerkten externen Zugriff
  - ➔ keine Begrenzung auf Durchsicht bestimmter Daten

- **Problem: Abgrenzung zum Fernmeldegeheimnis**
  - Rechtsprechung des BVerfG: Fernmeldegeheimnis betroffen, sofern
    - Telekommunikationsvorgang nicht abgeschlossen ist
    - Inhalt nicht durch „Empfänger“ beherrscht wird
  - Problem: Speicher bei TK-Anbieter z. B. Webmail-Account
  - Problem?: TK-Verbindung erforderlich zur externen Abfrage
- **„Online-Durchsuchung“ – Stichwort „Bundestrojaner“**
  - Gesetzesbegründung: keine Legitimation durch § 110 Abs. 3 StPO n. F.
  - Problem: keine Verankerung in Wortlaut des § 110 Abs. 3 StPO n. F
  - Problem: „Ausweitungstendenz“ der „StPO-Rechtsprechung“

Danke für die Aufmerksamkeit!

JUCONOMY Rechtsanwälte
Graf-Recke-Straße 82
40239 Düsseldorf

Kostenloser monatlicher Newsletter unter: www.juconomy.de