Telekommunikationsüberwachung TKÜ

TK = Technischer Vorgang des Aussendens, Übermittelns und Empfangens von Zeichen, Sprache, Bildern oder Tönen mittels techn Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können (vgl. § 3 Nr. 22, 23 TKG). Es werden auch die mit dem Versenden und Empfangen von Nachrichten mittels TK-Anlagen in Zshg stehenden Vorgänge erfasst (BGH NStZ 03, 668).

Bestandsdaten - Verkehrsdaten

- Bestandsdaten: § 95 TKG (Recht zur Speicherung); § 111 TKG (Pflicht zur Erhebung und Speicherung durch Provider)
- Bestandsdaten =
  - Name und Anschrift des Nutzers,
  - Geburtsdatum,
  - überlassene Rufnummern,
  - Gerätenummer der dem Nutzer überlassenen Mobilfunkendgeräte,
  - Datum des Vertragsbeginns
  - bei Festnetzanschlüssen: Anschrift, an welcher dieser Anschluss betrieben wird

Verkehrsdaten - § 96 TKG

- die Nummer/ Kennung, personenbezogene Berechtigungskennungen, bei Kundenkarten: Kartennummer, bei mobilen Anschlüssen: Standortdaten
- Beginn und Ende der jeweiligen Verbindung (Datum und Uhrzeit) soweit abrechnungsrelevant: Datenmengen
- genutzter Telekommunikationsdienst
- Bei festgeschalteten Verbindungen, (Beginn und Ende nach Datum und Uhrzeit), soweit abrechnungsrelevant: Datenmengen
- sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten

Bestandsdaten - Verkehrsdaten

Bestandsdaten Bsp: Name Anschluss-inhaber	Verkehrsdaten Bsp: Anrufverbindungen	
Eingriffsgrundlage: § 100j I 1 StPO iVm §§ 113, 95, 111 TKG (Ausnahme: dym IP-Adresse)	Verkehrsdaten für Abrechnung § 100g StPO, § 96 TKG / §§ 100j StPO iVm 113 TKG, Dyn. IP-Adresse	Vorratsdaten-speicherung § 100g StPO, § 113a,b TKG (Neuregelung – Anwendung ausgesetzt!)
<u>Kein</u> Eingriff in Art. 10 GG	Eingriff in Art 10 GG	

§ 113 I 2 TKG *alte Fassung*

Frühere Regelung gem BVerfG Beschl. v. 24.1.2012 – 1 BvR 1299/05: Verfassungswidrig!

- Keine spezifische Norm zur Datenerhebung der Behörden - fehlende Bundeskompetenz „Doppeltürenmodell“ = Norm zur Datenübermittlung und Norm für Abfrage

- Dynamische IP-Adressabfrage setzt Sichtung der Art. 10 GG unterfallenden Verbindungsdaten voraus -> Zitiergebot verletzt

Reform mit Wirkung zum 1.7.2013

Vgl. BT-Drucksache 17/12034

- § 100j StPO (→ Ermittlungsbehörde)

- § 113 TKG (→ Provider)

→ Doppeltürenmodell umgesetzt

§ 100j StPO - Überblick

→ Ermitteln, Speichern durch Provider

- 3 Eingriffsgrundlagen:
  - Abs. 1 Satz 1 (Bestandsdaten)
  - Abs. 1 Satz 2 (Zugangscode)
  - Abs. 2 (Dynamische IP-Adresse)

§ 113 TKG - Überblick

→ Ermitteln, Speichern durch Provider

- Bestandsdaten (§ 95, 111)/Zugangssicherungen durch manuelle Abfrage oder automatisierte Abfrage einschl. Ähnlichkeitssuche über gesamten Unternehmensdatenbestand
- Verkehrsdatenauswertung für dyn. IP-Adresse
- Pflicht des Providers zur Datenübermittlung und -sicherung sowie Verschwiegenheitspflicht

§ 100j Abs. 1 S. 1StPO

→ Ziel: Erforschung Sachverhalt oder Ermittlung Aufenthaltsort Beschuldigter

- Adressat: Provider
- Bestandsdaten (aber keine Verbindungsdaten)
- Verhältnismäßigkeit

  Norm entspricht allg. Generalklausel

  Kein Richtervorbehalt; keine Benachrichtigungspflicht

§ 100j Abs. 1 S. 2 StPO

→ Zugangssicherungscode (bspw PIN, PUK)

- Voraussetzungen für nachfolgende Verwendung (bspw Auslesen Adressbuch → § 94, 98 analog; Zugriff auf Kommunikation → § 100a)
- Adressat: Provider
- Zugangssicherung für Daten auf Endgerät oder externe Speichermedien (bspw Cloud)
- VHM /Grundrechtseingriff

§ 100j Abs. 2 – dynamische IP-Adressen

→ Ermittlung Sachverhalt / Aufenthaltsort Besch. (konkreter Straftatverdacht)

- Voraussetzungen entspr Abs. 1 S. 1 oder 2
- Kein Richtervorbehalt
- Adressat: Provider
- Datenabfrage bezogen auf bestimmte (dyn. vergebene) IP-Adresse, d.h. zu genau definiertem Zeitpunkt – nicht ggü Nichtverdächtigen → keine Abfrage in einem Zeitfenster.
- Wohl auch: Abfrage der IP-Adresse zu einem Account
- Nicht: Verdachtsunabhängige Abfrage von IP-Adressen

§ 100j Abs. 1 S. 2 (PUK) – Formelle Rechtmäßigkeit

- Abs. 3: Richtervorbehalt, auf Antrag StA. Sonderfall: Gefahr im Verzug (StA/ Ermittlungsbeamte) mit unverzüglicher Bestätigung
- Ausnahme: Richterlicher Beschluss liegt vor oder Betroffener hat Kenntnis /muss Kenntnis nehmen mit Dokumentation in Ermittlungsakte

§ 100j IV - Benachrichtigungspflicht

- Abfrage nach Abs. 1, Satz 2 oder Absatz 2 (nicht bei Abfrage nach Abs. 1 S. 1)
- Pflicht zur Benachrichtigung des Betroffenen
- Ausn: Keine Benachrichtigung,
  - soweit Zweck der Maßnahme gefährdet /vereitelt oder
  - Schutzwürdige Belange Dritter /Betroff. stehen entgegen
  - Aktendoku über Ausnahmevoraussetzungen

Rechtsschutz § 100j

- Keine eigene Prüfung des Providers (Bindung an richterliche Entscheidung)
- Betroffener kann *analog* § 101 Abs. 7 bzw. § 304 gg Beschluss Beschwerde einlegen
- Str, ob Frist von 2 Wochen nach Benachrichtigung einzuhalten, da § 100j in § 101 nicht aufgeführt.

§ 100i: IMSI-Catcher

- 1. Alt: Ermittlung einer Gerätekennung IMEI (International Mobile Equipment Identity) eines Mobiltelefons bzw. Ermittlung der Kennung einer SIM-Karte IMSI (International Mobil Subscriber Identity).
- 2. Alt: Ermittlung eines aktuellen Standortes des eingeschalteten Mobiltelefons in der Umgebung, wenn IMEI, IMSI oder Telefonnummer bekannt.

-> isoliert möglich oder zur Vorbereitung TKÜ / Erstellung Bewegungsprofil (§ 163f).

BVerfG

Beschl v. 22.08.2006 – 2 BvR 1343/03

Durch die Maßnahme werden alle Handys in der Gegend erfasst und in gewissem Umfang auch die Abwicklung von TK-Diensten verlangsamt. -> Eingriff in Art. 2 I iVm 1 I GG.
Gleichwohl ist die Norm verfassungsgemäß, da der Gesetzgeber ein hochrangiges Ziel verfolgt und die Maßnahme mit grundrechtssichernden Schranken versehen hat.

➔Voraussetzungen § 100i

- Ermittlungsziel: Erforschung des Sachverhalts oder des Aufenthaltsortes des Beschuldigten durch Geräte- / Kartennummer oder Standort eines Handy, auch zur Vorbereitung für § 100a

- Verdacht: Straftat von erheblicher Bedeutung
- Erforderlichkeit für das Ermittlungsziel.
- Betroffene: Auch Dritte, soweit unvermeidlich – begrenzte Verwendung: Abs. 2
- Verhältnismäßigkeit / Grundrechte

- ✓ Anordnungsbefugnis: Richter ausn. StA
- ✓ Dauer: Bis zu 6 Monate mit Verlängerungsmögl
- ✓ Formale Anforderungen entspr § 100e.

§ 100 g

§ 100g regelt die Übermittlung von Verkehrsdaten.

§ 100 g dient der Vorbereitung einer TKÜ, kann allerdings auch isoliert angewendet werden.

§ 100g: → Pflicht zur Auskunft über TK-Verbindungsdaten bei TK-Unternehmen.

§ 100g StPO

§ 100g Abs 1 Satz 1 StPO a.F. war verfassungswidrig, soweit er sich auf die Vorratsdatenspeicherung (§§ 113a, 113b TKG) bezog (BVerfG Urteil v. 2.3.2010 - 1 BvR 256/08):
Unverhältnismäßiger Eingriff in Art. 10 GG, da Gesetzgeber keine ausreichenden Sicherungen vorgesehen hatte.
Unabhängig von der Vorratsdatenspeicherung war § 100 g StPO anwendbar für die Verkehrsdaten, welche für die Vertragsabwicklung (Abrechnung) von den Unternehmen, dh unabhängig von §§ 113a f TKG gespeichert werden.

EU-Richtlinie zur Vorratsdatenspeicherung

- EuGH, Urt. v. 8.4.2014 – C 293/12 + C 594/12: EU-RiLi 2006/24/EG und geänderte RiLi 2002/58/EG sind **ungültig**!
- Ungültige RiLi: Vorgabe für Mitgliedsstaaten, Regelungen zu schaffen, wonach Provider Daten, insb Verbindungsdaten, für Zeitraum von mind. 6 Mon – 2 Jahren zu speichern haben.
- Unverhältnismäßiger Eingriff in GrundR der gesamten Bevölkerung (Gerichtliche Kontrolle; Umfang der Speicherung; Differenzierung zwischen Datenkategorien; fehlende Festlegung der Zwecke; Missbrauchsrisiko)
  → Keine Pflicht zur Umsetzung; nationale Neuregelung bleibt möglich.

➔§ 100g Abs. 1 Nr. 1:

- Ermittlungsziel: Verkehrsdaten, einschließlich Standortdaten in Echtzeit; nicht Vergangenheit → Abs. 2 n.F., aber Übergangsfrist gem. § 12 EGStPO Juli 2017
  - Verdacht auf Grund von Tatsachen
  - Straftat von – auch im Einzelfall - erheblicher Bedeutung, insb § 100a Abs. 2
  - Erforderlichkeit für Ermittlung des Sachverhalts oder des Aufenthaltsortes.
  - Verhältnismäßigkeit / Grundrechte
  - Formale Anforderungen entspr. §§ 100e; ausr zeitlich / räumlich Bezeichnung der TK

➔§ 100g Abs. 1 Nr. 2

- Ermittlungsziel: Verkehrsdaten gem § 96 TKG, mit Ausnahme der Echtzeitübertragung von Standort-daten.
  - Verdacht auf Grund von Tatsachen: Straftat mittels TK begangen (Abs. 1 Nr. 2)
  - Ermittlung von Sachverhalt oder Aufenthaltsort auf andere Weise aussichtslos.
  - Datenerhebung in angemessenem Verhältnis zur Tat / Grundrechte
  - Formale Anforderungen entsprechend § 101a iVm § 100e.

Funkzellenabfrage § 100g Abs. 3

- → Abfrage aller Verkehrsdaten, die in einer Funkzelle angefallen
- Voraussetzungen gem § 100g Abs. 1 Nr. 1
- Zusätzl gem § 100g Abs. 2, wenn Vorratsdaten
- VHM
  - Geeigent
  - Subsidarität: Aussichtslos/ wesentl erschwert
  - Angemessenheit, insb Kernbereichsschutz, vgl auch Abs. 4
- Form RM: → § 101a (Richtervorbeh)

§ 113a, b TKG; § 100g Abs. 2 - 4

- Gesetzgeber hat Vorratsdatenspeicherung neu geregelt (Gesetz v 10.12.2015 BGBl I S. 2218)
- § 113b TKG Speicherung von
  - Verbindungsdaten → 10 Wochen
  - Standortdaten (sms mit Inhalt; keine emails) → 4 Wochen
- Verpflichtet gem § 113a: TK-Anbieter; nicht kurzfristige Nutzung (hotspot)
- Praxis: Umsetzungsfrist für §§ 113b-e; 113g durch TK-Anbieter bis 1.7.2017; Sanktionierung **vorläufig ausgesetzt** OVG NRW 13 B 238/17; Hauptsache: BVerwG 6 C 12.18; vorgelegt: EuGH - C-793/19
- Verfassungsgerichtliche Prüfung ist zu erwarten

§ 100g Abs. 2

→ Erforschung SV; → Aufenthaltsort Täter/ Teilnehmer

- Anfangsverdacht bzgl Katalogtat gem Satz 2 (besonders schwere Straftat)
- Im Einzelfall besonders schwerwiegende Tat
- Subsidarität: wesentl erschwert/ aussichtslos
- Verhältnismäßigkeit (Angemessen)
- Unzulässig bei ZVR gem. § 53 I; § 160a III; IV

→ Erhebung Verkehrsdaten gem. § 113b TKG

Formelle Rechtmäßigkeit § 100g

- § 101a → § 100a III, § 100e: Richtervorbehalt; nur 100g I bei Gefahr iV: StA mit Bestätigung binnen 3 Werktagen
- Schriftlicher Beschluss mit:
  - Name, Adresse Betroffener
  - Rufnummer oder andere Kennung
  - Zu übermittelnde Daten, Art, Umfang, Zeitraum
- Mitwirkungspflicht TK-Anbieter mit Angabe der nach § 113b TKG vorratsgespeicherten Daten
- Unverzügliche Beendigung bei Fehlen der Voraussetzungen

Formelle Rechtmäßigkeit § 100g

- Befristung: 3 Monate mit Verlängerungsoption je max 3 Monate
- Bei Verlängerung: Einzelfallbezogener Beschluss
- Kennzeichnung der Daten, insb für gem. § 113b TKG und unverzügliche Auswertung
- Datenlöschung nach Abschluss

Verwendungsbegrenzung

- Verwendungsbeschränkung § 101a:
  - In anderen Strafverfahren → Katalogtat gem. § 100g
  - Präventiv: Abwehr konkr Gef für Leib, Leben, Freiheit Person; Bestand Bund / Land
- Übermittlung/ Verwendung präventiv erlangter Verkehrsdaten nur unter Voraussetzung § 100g (Katalogtat)

Benachrichtung, Löschung; Statistik

- § 101a: Benachrichtigung gem. § 101 der Beteiligten der TK, es sei denn unerheblich Mitbetroffene oder Gefährdung der weiteren Ermittlungen
- Zurückstellung der Benachrichtigung: Richtervorbehalt; Frist bei erstmaliger Zurückstellung max. 12 Monate
- Jährliche Stastik: → § 101b

Neuregelung v. 24.8.2017

- Quellen-TKÜ → § 100a Abs. 1: Zulassung von techn Mitteln zum Eingriff in informationstechnologische Systeme, wenn notwendig zur Überwachung bei verschlüsselter TK, soweit diese bei laufender, unverschlüsselter TKÜ angefallen wären; bspw Skype.
- Onlinedurchsuchung → § 100b: Eingriff in informationstechn System und umfassende Datenerhebung bei besonders schwerer Tat.

Überblick: § 100a Telekommunikationsüberwachung

- Abs 1, Satz 1: Überwachung / Aufzeichnung TK – Ausleitung durch den Provider („klassische“ TKÜ)
- Abs. 1, Satz 2: Quellen-TKÜ – Angriff auf das IT-System, bspw Trojaner zur Überwachung/ Aufzeichnung *laufender* Kommunikation vor der Verschlüsselung
- Abs. 1, Satz 3: Quellen-TKÜ bzgl *gespeicherter* Inhalte und Umstände der Kommunikation

§ 100a Abs. 1, S 1
Mat Rechtmäßigkeit, Teil 1

→ Aufzeichnung / Überwachung TK (auch) ohne Wissen Betroffener

Ziel: Aufklärung SV / Aufenthaltsort Beschuld.

- Tatverdacht bzgl schwerer Straftat (→ Katalogtat gem Abs. 2)
- Im Einzelfall schwerwiegende Tat
- Abs. 3: Beschuldigter/ Dritte: Nachrichtenmittler oder Anschlussinhaber eines dem Beschuldigten überlassenen Anschlusses.

§ 100a Abs. 1, S 1 Mat Rm Teil 2

- VHM: - Geeignetheit für Aufklärung SV/ Aufenthaltsort
  - Subsidaritätsklausel: auf andere Weise wesentl erschwert/ aussichtslos
  - Angemessen:
    - Eingriff in Art. 10 GG vs Aufklärungsinteresse schwerer Tat
    - inhaltliche Grenzen der Überwachung:
      - Kernbereich privater Lebensgestaltung gem. § 100d Abs. 1: Prognose, dass nicht nur kernbereichsrelevante Information erhoben wird; Verwertungsverbot § 100d Abs. 2 - Kernbereich nicht betroffen bei Gespräch über Straftat (BGH 2 StR 244/18)
      - Grenze: insb Verteidiger: § 148 bzw (auch bei anderen Berufsgeheimnisträgern) § 160a StPO.

Quellen-TKÜ (§ 100a I 2, 3)

→ Aufzeichnung / Überwachung TK (auch) ohne Wissen Betroffener

- Verdacht bzgl im Einzelfall schwerer Katalogtat
- Infiltration IT-System, soweit notwendig für Erlangung unverschlüsselter Kommunikation
- Begrenzung auf laufende Übertragungsvor-gänge, aber auch gespeicherter Inhalte und Umstände der Kommunikation ab Beschluss – Kontrollüberlegung: Hätte unverschlüsselte TKÜ gleiches Ergebnis gebracht
- Nur unerlässliche Systemeingriffe und techn mögliche Rückgängigmachung (Abs. 5)
- Weitere Voraussetzungen wie Abs. 1

Sonderprobleme

Mailverkehr:
- Gespeicherte Mails (§§ 94, 98 analog);
- Datenverkehr → Provider → §§ 100a, b.

Str, ob § 100 a entsprechend anwendbar für Zugriff auf zugangsgeschützte Bereiche im Internet. Vorzugswürdig: VE/ noeP

Str, ob anwendbar für das heimliche Abhören des nichtöffentlich gesprochenen Worts außerhalb des Fernmeldeverkehrs oder Verwertung von Raumgesprächen (dafür: BGH StV 03, 483). (P) Quellen-TKÜ mit Kameraaufnahme? (vgl § 100c)

Ob der Betroffene Kenntnis von der Maßnahme erlangt, ist nicht relevant.

Form Rm TKÜ → § 100e

- Antrag der Staatsanwaltschaft
- Anordnung durch Richter
- Sonderfall: Gefahr im Verzug: Staatsanwalt (nicht Ermittlungsbeamter) ordnet an und Richter bestätigt binnen 3 Tagen.
- Dauer: Max. 3 Monate. Mehrmalige Verlängerung um bis zu 3 Monate.
- Beschl: Schriflich mit Begründung (Abs. 3, 4)
- Berichtspflicht bzgl Ergebnis
- Online-DS: Protokollierung techn Mittel (§100a VI)

-> § 101

- § 101 IV 1 Nr. 3: Grds Benachrichtigungspflicht der TK-Teilnehmer und erheblich mitbetroffener Personen.
- Rechtsschutz: § 101 VII (vorrangig vor § 98 analog)
- Löschungspflicht: § 101 VIII nach Abschluss des Strafverfahrens mit Dokumentation.
- Zufallsfund → § ~~477 II 2~~. §§ 479 II1, 161 III
- Statistik: § 101b GenBA je zum 30.06.

§ 100b: Online-Durchsuchung

- Eingriff in Art. 2 Abs. 1 iVm 1 Abs. 1 GG: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Sonderfall ggü RiS, da Eingriffstiefe wesentlich größer.
- Reaktion auf zunehmend verschlüsselte Daten.
- IT-System: PC, Laptop, Handy, Tablet, …

§ 100b Mat Rm

→ (Heimliche) Online-Durchsuchung eines IT-Systems (auch retrograd)

- Ziel: Aufklärung SV/ Aufenthaltsort BS
- Gg BS oder ggü Dritten, wenn erforderlich (Abs. 3 Nr. 1, 2); Drittbetroffenheit soweit unvermeidb
- Verdacht bzgl besonders schw Tat (Abs. 2), die im Einzelfall bes schw wiegt

§ 100b Mat Rm

- Subsidaritätsklausel: wstl erschw/ aussichtsl
- Prognose: Nicht nur Kernbereichsrelevantes (§ 100d I); Löschung/Verwertungsverbot § 100d III
- § 100d V, ZVR-Berechtigte: § 53 - unzulässig; sonst abwägbar.
- VHM: Eingriff in 2 I, 1 I GG „IT-GrundR“ vs Aufklärungsinteresse

Zuständigkeit - Maßn gem § 100b

- Antrag der Staatsanwaltschaft
- Anordnung durch Kammer bei Landgericht
- Gefahr im Verzug: Vorsitzender Richter, Kammer bestätigt binnen 3 Tagen.
- Dauer: Max. 1 Monat. Mehrmalige Verlängerung um bis zu 1 Monat. Ab 6 Mon Gesamtdauer: OLG zuständig
- Beschl: Schriflich mit Begründung (Abs. 3, 4)
- Berichtspflicht bzgl Verlauf und Ergebnis
- Protokollierung techn Mittel gem § 100a VI

Verfahrensregelungen → § 101

- § 101 IV 1 Nr. 4: Grds Benachrichtigungspflicht der Zielperson und erheblich mitbetroffener Personen.
- Rechtsschutz: § 101 VII (vorrangig vor § 98 analog)
- Löschungspflicht: § 101 VIII nach Abschluss des Strafverfahrens und Dokumentation.
- Verwendungsbeschränkung für Zufallsfund: § 100e VI (vorrangig ggü § 161 III). Darf nicht als Spurenansatz dienen!
- Statistik gem § 101 b → GenBA

Zusammenfassung: Straftatenkataloge

- *Erhebliche* Straftat: Strafrahmenobergrenze mindestens 3 Jahre und geeignet das Gefühl der Rechtssicherheit und des Rechtsfriedens erheblich zu beeinträchtigen
- *Schwere* Straftat: Strafrahmenobergrenze mindestens 5 Jahre.
- *Besonders schwere* Straftat: Verbrechen mit Strafrahmenobergrenze von mindestens 10 Jahren.

TK-Überwachung

Eingriffsvoraussetzungen: Höher ↔ Niedriger
Tat: Besonders schw. ↔Schwere ↔ Erhebliche ↔ Jede
Anordnung: Richter/ StA Erm.beamte

§ 100g II Vorrats-Speicherung (Art. 10)

§ 100b Online-DS (2 I: IT-System)

§ 100a TK-Über-wachung + Aufzeich-nung

(Art. 10)

§ 100g I: Verkehrs-daten (Art. 10 / Art. 2 I)

§ 100i „IMSI-Catcher“ (str: nur Art. 2 I)

§§ 94 ff Beschlag-nahme

§ 100j (ggf. iVm spezieller Norm)

← Schwerer Grundrechtseingriff Leichter →
← Art. 10 GG / 2 I: IT-System →
← Art. 2 I, 1 I: RiS →