**Prof. Dr. Bernd Heinrich/Prof. Dr. Tobias Reinbacher** **Stand: 1. Oktober 2023**

**Examinatorium Strafprozessrecht – Arbeitsblatt Nr. 18**

# Überwachung der Telekommunikation – §§ 100a ff. StPO

**I. Allgemeines**: Die **Überwachung der Telekommunikation** (TKÜ) ist in § 100a StPO (Voraussetzungen) und § 100e StPO (Verfahren) geregelt. Diese **strafprozessuale Zwangsmaßnahme** (vgl. Arbeitsblatt Nr. 12) ist regelmäßig mit Grundrechtseingriffen verbunden, weswegen besondere Anforderungen an die Ermächtigungsgrundlage zu stellen sind. § 100a StPO gewährt sowohl einen Eingriff in die durch Art. 10 GG geschützte Privatsphäre des Beschuldigten als auch in die unbeteiligter Dritter (insbesondere der Gesprächspartner oder bestimmter Nachrichtenmittler; vgl. dazu unten II 8). § 100a StPO gestattet nicht nur die **Überwachung** der Telekommunikation, sondern darüber hinaus auch die **Aufzeichnung** der Gespräche durch die Ermittlungsbehörden. Dabei ist der Anwendungsbereich des § 100a StPO nicht nur auf die herkömmlichen Formen des Telefonierens und Fernschreibens beschränkt, sondern umfasst **jegliche Art der unverschlüsselten(!) Nachrichtenübermittlung**, z.B. auch in Form von SMS oder E-Mails, Messenger-Systemen und sämtlichen Arten der Internet-Telefonie (bei verschlüsselten Kommunikationen muss zumeist ein sog. Quellen-Telekommunikationsüberwachung durchgeführt werden, vgl. Arbeitsblatt Nr. 19). Zum Begriff der Telekommunikation vgl. **§ 3 Nr. 59 TKG**. Der Kernbereich privater Lebensgestaltung ist durch **§ 100d StPO** geschützt.

**II. Voraussetzungen der Überwachung der Telekommunikation, §§ 100a, 100e StPO**

1. Anordnungsbefugnis: Nach § 100e I StPO ist das Gericht auf Antrag der StA, bei Gefahr im Verzug auch die StA zuständig. Die Anordnung tritt in letzterem Fall außer Kraft, wenn nicht innerhalb von 3 Tagen eine richterliche Bestätigung ergeht (§ 100e I 3 StPO). Die Höchstdauer der erstmaligen Anordnung der Maßnahme beträgt 3 Monate, kann aber verlängert werden (§ 100e I 4, 5 StPO). Die Betroffenen sind von der Überwachung nachträglich zu benachrichtigen (§ 101 IV 1 Nr. 3 StPO).
2. Kernbereichsschutz: Es dürfen keine tatsächlichen Anhaltspunkte vorliegen, dass durch die Maßnahme allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, § 100d I StPO.
3. Vorliegen eines Tatverdachts, § 100a I 1 Nr. 1 StPO: Erfasst sind hierbei sowohl Täter als auch Teilnehmer; ferner sowohl Vollendungs- als auch Versuchstaten; ferner auch bestimmte Vorbereitungshandlungen. Der Verdacht muss aufgrund einer hinreichenden Tatsachenbasis ein gewisses Maß an Konkretisierung erreicht haben.
4. Katalogtaten: Die Anordnung der Telefonüberwachung ist nur bei Verdacht einer in § 100a II StPO genannten Katalogtat zulässig, § 100a I 1 Nr. 1 StPO.
5. Schwere der Tat auch im Einzelfall: Die Tat muss auch im konkreten Einzelfall schwer wiegen, § 100a I 1 Nr. 2 StPO.
6. Subsidiaritätsgrundsatz: Die Anordnung der Telefonüberwachung kommt nur dann in Betracht, „wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre", § 100a I 1 Nr. 3 StPO.
7. Verhältnismäßigkeit: Wie stets bei Zwangsmaßnahmen zu prüfen.
8. Betroffene Personen: Die Anordnung richtet sich in erster Linie gegen den Tatverdächtigen. Darüber hinaus kann die Telefonüberwachung auch unmittelbar gegen Dritte angeordnet werden, wenn der Verdacht besteht, dass diese für den Beschuldigten als **Nachrichtenmittler** fungieren (vgl. § 100a III StPO; hier ist auch näher umschrieben, wann eine solche Nachrichtenmittlerfunktion vorliegt).

**III. Sonderprobleme**

1. Zufallsfunde: Anlässlich einer Telefonüberwachung erlangte Informationen bzgl. anderer Taten dürfen nur verwertet werden, wenn es sich hierbei ebenfalls um eine der genannten Katalogtaten handelt, **§§ 161 III, 479 II 1 StPO**. Dem liegt der Gedanke des hypothetischen Ersatzeingriffs zu Grunde. Problematisch ist, ob allein das Vorliegen einer Katalogtat ausreicht (sog. abstrakte Betrachtung) oder ob darüber hinaus die sonstigen Voraussetzungen des § 100a StPO hypothetisch für das anhängige Verfahren zu prüfen sind (sog. konkrete Betrachtung). Der BGH hat dies offen gelassen (vgl. BGHSt 58, 32, (49)).
2. Verteidiger als „Nachrichtenmittler": Eine Ausnahme von der Möglichkeit der Überwachung Dritter nach § 100a III StPO ist dann zu machen, wenn der Verteidiger des Beschuldigten als Nachrichtenmittler in Betracht kommt, da sonst eine Umgehung der in § 148 StPO enthaltenen Rechtsgarantie des unüberwachten mündlichen Verkehrs zwischen Verteidiger und Beschuldigtem zu befürchten wäre. Dies gilt jedenfalls so lange, bis der Verteidiger nach § 138a I Nr. 1 StPO in dem Verfahren ausgeschlossen ist.
3. Hörfalle: Keine Überwachung im Sinne des § 100a StPO liegt vor, wenn ein Anschlussbenutzer der Polizei das Mithören eines Telefongesprächs gestattet, ohne dass der Gesprächspartner davon Kenntnis hat, denn in diesen Fällen gilt das Fernmeldegeheimnis nicht (vgl. Arbeitsblatt Nr. 31).
4. Abrufen von E-Mails: Hier muss wie folgt differenziert werden: Während des **Sende- oder Abrufvorganges** gilt § 100a StPO; sind die E-Mails beim **Beschuldigten gespeichert**, ist nur die Beschlagnahme des Datenträgers nach § 94 StPO möglich; sind sie noch **beim Provider**, so war dies bislang **sehr str.**, nach t.v.A. sollte § 100a StPO gelten; nach Entscheidung des **BGH NJW 2009, 1828**, ist jedoch in letzterem Fall **nicht** § 100a StPO, sondern **§ 99 StPO** anwendbar; ebenso auch BVerfGE 124, 43. Der **BGH** hat nun entschieden, dass bei „ruhenden" Emails, die beim Provider (zwischen-)gespeichert sind, ein heimliches Vorgehen auf Grundlage von § 100a I 1 StPO neben § 94 StPO möglich ist; die Maßnahmen sollen sich ergänzen (NStZ 2021, 355).
5. IMSI-Catcher bei Handys: Gemäß § 100i StPO dürfen auch sog. International-Mobile-Subscriber-Indentity-Catcher eingesetzt werden, mithilfe derer die Geräte- und Kartennummer sowie der Standort des Handys ermittelt werden; nach **BVerfG NJW 2007, 351**, ist hierdurch nicht Art. 10 GG, sondern allenfalls das Recht auf informationelle Selbstbestimmung und die allgemeine Handlungsfreiheit betroffen.
6. Versenden einer stillen SMS: Hierunter versteht man das Versenden (einer Vielzahl) von Kurzmitteilungen an das Handy des Beschuldigten, die eine Rückmeldung des Mobiltelefons bei der nächsten Funkzelle auslösen, jedoch im Nachrichteneingang des Handys nicht angezeigt werden. Ziel ist die Erstellung eines Bewegungsprofils des Beschuldigten. Die Ermächtigungsgrundlage für das Versenden derartiger stiller SMS ist streitig. Nach Ansicht des BGH ist sie in § 100i I Nr. 2 StPO zu finden (**BGH NStZ 2018, 611**). Zuvor wurde in der Praxis § 100a i.V.m. den §§ 161 I 1, 163 I StPO herangezogen. Andere Stimmen stellten direkt auf § 100a StPO oder auf § 100h I 1 Nr. 2 StPO ab.
6. Auskunftspflicht der Telekommunikationsbetreiber: Gemäß § 100a IV StPO müssen die Telekommunikationsbetreiber den Ermittlungsbehörden die Maßnahmen nach § 100a StPO ermöglichen und die erforderlichen Auskünfte erteilen. Die Erhebung von **Verkehrsdaten** (d.h. nicht betreffend den Inhalt der Telekommunikation, sondern Telefonnummern und Zeiten des Gesprächs) erfolgt nun gemäß **§ 100g StPO**.

**Literatur/Lehrbücher:** *Heinrich/Reinbacher*, Examinatorium Strafprozessrecht, 4. Auflage 2023, Problem 18.
**Literatur/Aufsätze:** *Freiling/Rückert/Safferling*, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9; *Jahn*, Der strafprozessuale Zugriff auf Telekommunikationsverbindungsdaten, JuS 2006, 491; *Kudlich*, Persönlichkeitsschutz für einen Handy-Dieb – keine Auskunft über Telekommunikation mit einem gestohlenen Handy, JA 2009, 72; *Roggan*, Der Schutz des Kernbereichs privater Lebensgestaltung bei strafprozessualer Telekommunikationsüberwachung, StV 2011, 762; *ders.*, Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen, NJW 2015, 1995.
**Literatur/Fälle:** *Keiser*, Immer Ärger mit E-Mails, JA 2001, 662.
**Rechtsprechung:** **BVerfG NJW 2006, 976** – Bargatzky (Zugriff auf Verbindungsdaten); **BVerfG NJW 2007, 351** – Handy (Art. 10 GG nicht betroffen); **BVerfG NJW 2009, 1405** – Rasterfahndung (Abfrage von Kreditkartendaten); **BVerfG NJW 2009, 2431** – E-Mail (Beschlagnahme von E-Mails); **BVerfG NJW 2010, 833** – Vorratsdatenspeicherung (Verfassungswidrigkeit); **BVerfG NJW 2012, 833** – verdeckte Ermittlungsmaßnahmen (Verfassungsmäßigkeit); **BVerfG NJW 2019, 584** – Nichtannahmebeschluss (zu den Mitwirkungs- und Vorhaltungspflichten eines TK-Anbieters im Rahmen einer TKÜ); **BGHSt 33, 347** – Strafverteidiger (TKÜ bei Verteidiger); **BGHSt 39, 335** – Hörfalle (Mithören mit Zustimmung des Anschlussinhabers); **BGHSt 51, 1** – Abhörkette (Zufallsfunde bei TKÜ); **BGHSt 53, 64** – Zufallsfunde (Verwertbarkeit bei Änderung der Anordnungsvoraussetzungen); **BGH NStZ 1997, 247** – Mailbox (Anwendungsbereich erfasst andere Formen der Nachrichtenübermittlung); **BGH StV 2001, 214** – Handy (Erstellung von Bewegungsprofilen); **BGH NJW 2003, 234** – Handyfehlbedienung (Verwertbarkeit eines Gesprächs nach Handy-Fehlbedienung); **BGH NJW 2009, 1828** – E-Mail (Beschlagnahme von E-Mails); **BGH StV 2017, 434** – TKÜ (Anforderungen an Tatverdacht); **BGH NStZ 2018, 550** – Hintergrundgeräusche (Verwertung aufgezeichneter Hintergrundgeräusche und -gespräche); **BGH NJW 2018, 2809** – „Stille SMS" (Rechtsgrundlage für Versenden sog. „stiller SMS" durch Ermittlungsbehörden ist § 100i I Nr. 2 StPO), vgl. *Maihöfer/Wingenfeld*, famos 12/2018; **BGH NStZ 2021, 355** – zum Zugriff auf beim Provider zwischen- oder endgespeicherte („ruhende") Emails.