Sachstand

Überwachung von Kommunikation zu repressiven und präventiven Zwecken

Kurzübersicht

Rechtlicher Rahmen der Überwachung von Kommunikation zum Zwecke der Strafverfolgung und Gefahrenabwehr

Aktenzeichen:	WD 7 - 3000 - 016/23, WD 3 - 3000 - 025/23
Abschluss der Arbeit:	27.02.2023
Fachbereiche:	WD 7: Zivil-, Straf- und Verfahrensrecht, Bau und Stadtentwicklung (Gliederungspunkt 1) WD 3: Verfassung und Verwaltung (Gliederungspunkt 2)

1. Repressive Abhörmaßnahmen

Abhörmaßnahmen zum Zweck der Strafverfolgung – also zu repressiven Zwecken – werden in der Strafprozessordnung[1] (StPO) geregelt. Dort wird zwischen der akustischen Überwachung innerhalb (§ 100c StPO) und außerhalb (§ 100f StPO) von Wohnraum sowie der Telekommunikationsüberwachung (§ 100a StPO) unterschieden.

Telekommunikationsüberwachung und die akustische Überwachung außerhalb von Wohnraum dürfen nur bei dem Verdacht einer schweren Straftat angeordnet werden (§§ 100a Absatz 1 Satz 1 Nr. 1, Absatz 2, 100f Absatz 1 StPO). Wohnraumüberwachungen setzen sogar den Verdacht einer besonders schweren Straftat voraus (§ 100c Absatz 1 Nr. 1 StPO). Ferner ist für die Telekommunikationsüberwachung und die akustischen Überwachung außerhalb von Wohnraum erforderlich, dass die Tat im Einzelfall schwer wiegt (§§ 100a Absatz 1 Satz 1 Nr. 2, 100f Absatz 1 StPO). Im Fall der Wohnraumüberwachung muss die Tat im Einzelfall besonders schwer wiegen (§ 100c Absatz 1 Nr. 2 StPO). Für alle Maßnahmen gilt, dass sie erst nachrangig angeordnet werden dürfen, wenn die Erforschung des Sachverhalts, die Ermittlung des Aufenthaltsorts des Beschuldigten oder die Ermittlung des Aufenthaltsorts eines Mitbeschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wären (§§ 100a Absatz 1 Satz 1 Nr. 1, 100c Absatz 1 Nr. 4, 100f Absatz 1 StPO). Eine akustische Wohnraumüberwachung darf darüber hinaus nur angeordnet werden, wenn davon auszugehen ist, dass durch die Überwachung tatsächlich Äußerungen des Beschuldigten erfasst werden (§ 100c Absatz 1 Nr. 3 StPO). Alle dargestellten Ermittlungsmaßnahmen sind schließlich unzulässig, wenn Anhaltspunkte dafür vorliegen, dass durch sie allein Erkenntnisse aus dem Kernbereich der privaten Lebensgestaltung erlangt werden (§ 100d Absatz 1 StPO, § 100f Absatz 4 StPO i.V.m. §100d Absatz 1 StPO).

Verfahrensrechtlich sind die Telekommunikationsüberwachung und die akustische Überwachung außerhalb von Wohnraum grundsätzlich durch ein Gericht anzuordnen. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden – eine solche Anordnung bedarf jedoch der gerichtlichen Bestätigung binnen drei Werktagen (§ 100e Absatz 1 Satz 1 und 2 StPO, § 100f Absatz 4 StPO i.V.m. § 100e Absatz 1 Satz 1 und 2 StPO). Die akustische Wohnraumüberwachung bedarf dagegen in jedem Fall einer gerichtlichen Anordnung (§ 100e Absatz 2 Satz 1 StPO). Die Anordnung der Telekommunikationsüberwachung und der Akustischen Überwachung außerhalb von Wohnraum ist grundsätzlich auf höchstens drei Monate zu befristen und kann um nicht mehr als jeweils drei Monate verlängert werden (§ 100e Absatz 1 Satz 4 und 5 StPO, § 100f Absatz 4 StPO i.V.m. § 100e Absatz 1 Satz 4 und 5 StPO). Die Akustische Wohnraumüberwachung ist hingegen grundsätzlich auf die Dauer von einem Monat zu begrenzen und kann um nicht mehr als einen Monat verlängert werden (§§ 100e Absatz 2 Satz 4 und 5, 100f Absatz 4 StPO). Für alle Maßnahmen gilt, dass die durch die Überwachung erlangten Daten unverzüglich zu löschen sind, wenn sie zur Strafverfolgung oder zur gerichtlichen Überprüfung der Maßnahmen nicht mehr benötigt werden (§ 101 Absatz 8 StPO). Die betroffenen

1 Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 25. März 2022 (BGBl. I S. 571) geändert worden ist, in deutscher Sprache abrufbar unter: https://www.gesetze-im-internet.de/stpo/BJNR006290950.html. Englische Übersetzung mit Stand vom 22. November 2021 abrufbar unter: https://www.gesetze-im-internet.de/englisch_stpo/index.html (Stand dieser und sämtlicher nachfolgenden Internet- Quellen: 27. Februar 2023).

Personen sind nach der Beendigung der verdeckten Ermittlungsmaßnahme zu benachrichtigen (§ 101 Absatz 4 Satz 1 Nrn. 3, 5, 6 StPO).

Für die Strafverfolgungsbehörden gilt eine Pflicht zur gesonderten Aktenführung („Sonderhefte“[2]) für die akustische Wohnraumüberwachung und für die Überwachung außerhalb von Wohnraum gemäß § 101 Absatz 2 StPO (vgl. auch § 68 Absatz 4 Satz 3 und 4 StPO). Die zu den Sonderheften genommenen Erkenntnisse und die zur Speicherung verwendeten Datenträger können nach ihrer Offenlegung durch die Betroffenen und ihre Verteidiger nach den allgemeinen Grundsätzen der Akteneinsicht (§ 147 StPO) eingesehen werden[3]; gleiches gilt auch für die im Rahmen der Telekommunikationsüberwachung erlangten Daten.[4]

Daten, die durch eine Telekommunikationsüberwachung oder akustische Überwachung außerhalb von Wohnraum gewonnen wurden, dürfen in anderen Strafverfahren nur zur Aufklärung solcher Straftaten verwendet werden, die für sich genommen auch die Anordnung einer solchen Maßnahme hätten rechtfertigen können (§ 479 Absatz 2 Satz 1 StPO i.V.m. § 161 Absatz 3 StPO). Auch zur Gefahrenabwehr dürfen diese Daten durch andere Behörden nur dann verwendet werden, wenn eine entsprechende Maßnahme auch nach den gesetzlichen Grundlagen der Gefahrenabwehr hätte angeordnet werden dürfen (§ 479 Absatz 2 Satz 2 Nr. 2 StPO). Zur Abwehr anderer Gefahren, etwa für die Gesundheit, bedeutende Vermögenswerte oder die staatliche Sicherheit, darf auf die Daten einer Telekommunikationsüberwachung oder einer akustischen Überwachung außerhalb von Wohnraum zugegriffen werden, wenn sich aus den Daten im Einzelfall jeweils konkrete Ansätze zur Abwehr einer solchen Gefahr erkennen lassen (§ 479 Absatz 2 Satz 2 Nr. 2 StPO). Daten, die durch eine akustische Wohnraumüberwachung gewonnen wurden, dürfen in anderen Strafverfahren nur zur Aufklärung von Straftaten verwendet werden, die selbst die Anordnung einer solchen Maßnahme hätten rechtfertigen können (§ 100e Absatz 6 Nr. 1 StPO). Zur Gefahrenabwehr darf auf diese Daten nur bei einer bestehenden Lebensgefahr oder einer dringenden Gefahr, etwa für die Gesundheit, die staatliche Sicherheit oder bedeutende Vermögenswerte, zugegriffen werden (§ 100e Absatz 6 Nr. 2 StPO).

Die nach §§ 100a, c, f StPO angeordneten Maßnahmen werden im Rahmen des Ermittlungsverfahrens durch die ermittelnde Polizeibehörde durchgeführt. §§ 100c Absatz 1, 100f Absatz 1 StPO gestatten das Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes mit „technischen Mitteln“. Um welche technischen Mittel es sich dabei handelt, hat der Gesetzgeber bewusst offengelassen, um den Strafverfolgungsbehörden die Möglichkeit zu geben, entsprechend der technologischen Entwicklung auf diejenige Technik zurückgreifen zu können, die für die konkrete Maßnahme am geeignetsten erscheint.[5] Die technischen Mittel dürfen indes allein zur Sprachaufzeichnung eingesetzt werden: Nicht statthaft ist der Einsatz technischer Mittel in

---

2 Hegmann, in: Beck´scher Online Kommentar zur Strafprozessordnung, 46. Edition (Stand: 01.01.2023), § 101 StPO, Rn. 4.

3 Hegmann a.a.O. Rn. 5.

4 Hegmann a.a.O. Rn. 5.

5 Rückert, in: Münchener Kommentar zur Strafprozessordnung, 2.Auflage 2023, Band 1, § 100c StPO, Rn. 54 und § 100f StPO, Rn. 33.

Wohnungen zur Herstellung von Fotos oder Videoaufzeichnungen.[6] Neben dem eigentlichen Einsatz der „technischen Mittel“ gestattet die Vorschrift auch alle damit notwendiger Weise einhergehenden Begleitmaßnahmen wie das wiederholte heimliche Betreten der Wohnung zum Zwecke des Ein- bzw. Ausbaus der Technik.[7] Für die Telekommunikationsüberwachung, die heute größtenteils im Internet verschlüsselt erfolgt, erlaubt § 100a Absatz 1 Satz 2 StPO den Strafverfolgungsbehörden, mit Hilfe einer Überwachungssoftware, die den Anforderungen des § 100a Absatz 5 Satz 1 Nr. 1 lit. a StPO entsprechen muss, eine von dem Betroffenen und seinem/seinen Kommunikationspartner(n) verschlüsselt geführte Kommunikation in (noch) unverschlüsselter Form zu überwachen und aufzuzeichnen. Als Annexkompetenz dazu erlaubt § 100a Absatz 1 Satz 2 StPO gleichzeitig als ergänzende Maßnahme die Aufbringung von Entschlüsselungs- und Übertragungssoftware auf dem zu überwachenden Rechner.[8]

2. Präventive Abhörmaßnahmen

Die heimliche Überwachung der Telekommunikation und das Instrument der Online-Durchsuchung können auch zu präventiven Zwecken eingesetzt werden; die Telekommunikationsüberwachung allerdings in größerem Umfang als die Online-Durchsuchung.

Gesetzliche Ermächtigungsgrundlagen zur Telekommunikationsüberwachung finden sich in allen Polizeigesetzen der Länder sowie im Bundeskriminalamtgesetz (BKAG[9]). Auch die Nachrichtendienste des Bundes, also das Bundesamt für Verfassungsschutz, das Bundesamt für den Militärischen Abschirmdienst sowie der Bundesnachrichtendienst, können nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G 10[10]) unter bestimmten Voraussetzungen das Instrument der Telekommunikationsüberwachung einsetzen. Die Landesämter für Verfassungsschutz verfügen ebenfalls über entsprechende Ermächtigungsgrundlagen.

Vom Instrument der Onlinedurchsuchung darf auf Bundesebene das Bundeskriminalamt (BKA) Gebrauch machen sowie der Bundesnachrichtendienst, letzterer allerdings nur im Ausland und nur in Bezug auf ausländische Staatsangehörige (vgl. § 34 BNDG[11]). Dem Bundesamt für Verfas-

---

6 Rückert a.a.O. § 100c StPO, Rn. 54 und § 100f StPO, Rn. 34.

7 Rückert a.a.O. § 100c StPO, Rn. 54 und § 100f StPO, Rn. 35.

8 Graf, in: Beck´scher Onlinekommentar zur Strafprozessordnung, 46. Edition (Stand: 01.01.2023), § 100a StPO, Rn. 115.

9 Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch Artikel 3 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632) geändert worden ist, in deutscher Sprache abrufbar unter https://www.gesetze-im-internet.de/bkag_2018/.

10 Artikel 10-Gesetz vom 26. Juni 2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), das zuletzt durch Artikel 6 Absatz 4 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, in deutscher Sprache abrufbar unter https://www.gesetze-im-internet.de/g10_2001/.

11 BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist, in deutscher Sprache abrufbar unter https://www.gesetze-im-internet.de/bndg/.

sungsschutz und dem Militärischen Abschirmdienst steht dieses Überwachungsinstrument überhaupt nicht zur Verfügung. In einigen Bundesländern dürfen die Polizeibehörden das Mittel der Online-Durchsuchung einsetzen.

Die Überwachung der Telekommunikation unterliegt strengen verfassungsrechtlichen Vorgaben, die sich aus dem in Artikel 10 des Grundgesetzes (GG[12]) garantierten Brief-, Post- und Fernmeldegeheimnis ergeben. Noch strenger sind die Anforderungen an Online-Durchsuchungen. Denn diese greifen in das „Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme“ ein, welches das Bundesverfassungsgericht eigens für solche Maßnahmen aus dem allgemeinen Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG abgeleitet hat.[13]

Demzufolge eng sind die entsprechenden gesetzlichen Ermächtigungsgrundlagen ausgestaltet. Für das Bundeskriminalamt (BKA) ergeben sie sich aus § 49 BKAG und § 51 BKAG. Hiernach darf das BKA eine Online-Durchsuchung zum Beispiel durchführen, wenn „eine Gefahr vorliegt für […] Leib, Leben oder Freiheit einer Person oder […] solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt“ (§ 49 Absatz 1 Nr. 1 BKAG). Die Überwachung der Telekommunikation ist möglich, wenn „dies zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse liegt, geboten ist“ (§ 51 Absatz 1 Nr. 1 BKAG). Sowohl die Online-Durchsuchung als auch die Telekommunikationsüberwachung dürfen nur mit richterlicher Genehmigung durchgeführt werden (§ 49 Abs. 4, § 51 Absatz 3 BKAG). Nach Beendigung der Maßnahme sind die überwachten Personen grundsätzlich über diese zu unterrichten (vgl. § 74 Absatz 1 Nr. 6, 8 BKAG).

* * *

12 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2478) geändert worden ist. In deutscher Sprache abrufbar unter https://www.gesetze-im-internet.de/gg/, in englischer Sprache mit Stand 28. Juni 2022 abrufbar unter https://www.gesetze-im-internet.de/englisch_gg/index.html.

13 BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 – (http://www.bverfg.de/e/rs20080227_1bvr037007.html; auch auf Englisch).