Verbindungslinien zwischen Verfassungsrecht und strafprozessualen Ermittlungsmaßnahmen – Teil 2* Überlegungen anhand der verdeckten Maßnahmen der §§ 100a–100c StPO

*Akad. Rat a.Z. Dr. Pepe Schladitz, Osnabrück/Passau***

IV. Überblick über die einzelnen Ermittlungsbefugnisse der §§ 100 a–100c StPO

Die verdeckten Maßnahmen der §§ 100a ff. StPO regeln nach dem bisher Gesagten Eingriffe in die Privatsphäre des Betroffenen, deren Schutz im Einzelnen durch unterschiedliche Grundrechte ausformuliert wird.[1] Das soll nunmehr detaillierter herausgearbeitet werden.

1. Die Telekommunikationsüberwachung (TKÜ) gem. § 100a StPO

§ 100a StPO enthält in dessen Abs. 1 durchaus distinkte Ermächtigungsgrundlagen. Grund hierfür ist der verfassungsrechtliche Hintergrund: Die einzelnen Ermittlungsmaßnahmen greifen in divergierende Grundrechte ein.[2]

---

* Teil 1 ist in Ausgabe 2/2025 erschienen, Teil 3 folgt in Ausgabe 4/2025.

** Der *Autor* ist Akad. Rat a.Z. am Lehrstuhl für Strafrecht, Wirtschafts- und Steuerstrafrecht (Prof. Dr. *Roland Schmitz*) der Universität Osnabrück. Er vertritt im Sommersemester 2025 den Lehrstuhl für Strafrecht, Strafprozessrecht, Wirtschaftsstrafrecht und Strafrechtsgeschichte an der Universität Passau.

[1] Die nachfolgenden Überlegungen widmen sich demgegenüber nicht der weitergehenden bzw. anders gelagerten Frage, ob und in welchem Umfang im Ermittlungsverfahren öffentlich zugängliche Daten im Internet (bspw. aus sozialen Netzwerken) erhoben und verwertet werden dürfen. Hierzu ausf. *Rückert*, ZStW 129 (2017), 302.

[2] Vgl. *Rüscher*, NStZ 2018, 687 (689); *Grözinger*, GA 2019, 441 (452).

a) Wichtige Differenzierung: TKÜ und Quellen-TKÜ

Die Telekommunikationsüberwachung (TKÜ) gem. § 100a Abs. 1 S. 1 StPO legitimiert die heimliche Überwachung *laufender* Kommunikationsvorgänge unabhängig vom jeweiligen technischen Kommunikationsweg, also Telefonate, aber auch elektronische Bild- oder Textnachrichten.[3] Der konkrete technische Übertragungsweg ist somit unerheblich.[4] Der Begriff der Telekommunikation ist im Übrigen offen für technische Neuerungen.[5]

Zeitlich erfasst die TKÜ nur den *laufenden* Übertragungsweg und stellt sich aus diesem Grund als Eingriff in das Fernmeldegeheimnis gem. Art. 10 GG dar.[6] In technischer Hinsicht wird die TKÜ vor allem durch die Inpflichtnahme des Anbieters des Telekommunikationsdienstes realisiert.[7] Details hierzu regelt § 100a Abs. 4 StPO.

Gegenstand der TKÜ ist der Inhalt der Kommunikation (Kommunikationsdaten) sowie deren nähere Umstände, wie die Nummern der an der Kommunikation beteiligten Anschlüsse, Beginn und Ende die Menge der Kommunikation (Verbindungs- bzw. Verkehrsdaten, vgl. §§ 3 Nr. 70, 176 Abs. 2 TKG).[8]

Seit der Reform von 2017 legitimiert die StPO mit § 100a Abs. 1 S. 2 StPO nun auch *explizit* eine spezifische Form der Telekommunikationsüberwachung dergestalt, dass in die vom Betroffenen genutzten informationstechnischen Systeme mittels heimlich installierter Programme eingegriffen werden darf (sog. Quellen-Telekommunikationsüberwachung).[9] Die verfassungsrechtliche Zulässigkeit der Quellen-TKÜ ist im Grundsatz gegeben, wie das BVerfG zur gefahrenabwehrrechtlichen Parallelvorschrift des § 51 Abs. 2 BKAG festgestellt hat.[10] Das BVerfG hat in seinen Stellungnahmen zu gefahrenabwehrrechtlichen Online-Durchsuchungen Leitlinien vorgegeben, die bei der Kodifizierung des strafprozessualen Äquivalents zu berücksichtigen waren.[11]

Näherer Grund für diese spezielle Ermächtigungsgrundlage ist ein technischer Unterschied. Immer mehr Kommunikation erfolgt Internetprotokoll-(IP)-basiert. Kommunikation über „Voice-over-IP" und Messenger-Dienste wird zudem regelmäßig mit einer Verschlüsselung versehen. Der Zugriff auf diese Daten über ein öffentliches Telekommunikationsnetz wird vom Gesetzgeber als nicht prakti-

---

[3] *Beulke/Swoboda*, Strafprozessrecht, 16. Aufl. 2022, Rn. 390 f.; *Großmann*, JA 2019, 241; *Kindhäuser/Schumann*, Strafprozessrecht, 7. Aufl. 2023, § 8 Rn. 81; *Ostendorf/Brüning*, Strafprozessrecht, 5. Aufl. 2024, § 8 Rn. 54. Ausf. *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100a Rn. 11 ff.

[4] Siehe *Großmann*, JA 2019, 241; *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 1.

[5] *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 29.

[6] *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100a Rn. 1, 4; *Eidam*, NJW 2016, 3511 (3512); *Großmann*, JA 2019, 241; *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 3. Dezidiert *Heinrich*, ZIS 2020, 421 (422).

[7] Siehe *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 37 ff.; *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 33.

[8] *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 13 f., 61 f. Ausf. zu den verschiedenen Datenbegriffen siehe *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 69 ff. Zur in diesem Zusammenhang wichtigen Differenzierung zwischen Inhalts-, Verkehrs-, Bestands- und Nutzungsdaten, wie sie auch im TKG vorgenommen wird (§ 176 Abs. 1, Abs. 5, Abs. 6 TKG) siehe *Bär* ZIS 2011, 53 (55 f.); *Bantlin*, JuS 2019, 669.

[9] Zum vor der Reform geführten Streit um die Quellen-TKÜ siehe bspw. *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 96 ff.; *Roggan*, StV 2017, 821. Zum Ganzen auch *Großmann*, JA 2019, 241 (243). Der Gesetzgeber begreift die Neuregelung zur Quellen-TKÜ in § 100a Abs. 1 S. 2 und 3 auch als Klarstellung, BT-Drs. 18/12785, S. 49.

[10] BVerfG NJW 2016, 1781.

[11] Siehe BVerfG NJW 2008, 822; BVerfG NJW 2016, 1781. Siehe die pointierte Darstellung bei *Krusel/Grzesiek*, KritV 2017, 331 (340 ff.).

kabel qualifiziert, weil die Kommunikation aus den entsprechenden Systemen zwar in ein öffentliches Netz ausgeleitet werden könne, dann aber nur verschlüsselt vorliege. Die Entschlüsselung der entsprechenden Daten wäre zu zeitaufwendig oder gar gänzlich ausgeschlossen.[12] Deswegen komme nur ein „Ausleiten" der Informationen – namensgebend – „an der Quelle" *vor* der Verschlüsselung in Betracht.[13] Die Quellen-TKÜ betrifft (anders als die Online-Durchsuchung gem. § 100b StPO) laufende Kommunikation und ist somit als Ergänzung der regulären TKÜ konzipiert.[14] Die Quellen-TKÜ erlaubt es, die noch unverschlüsselten Daten, die im Laufe des Kommunikationsverlaufs verschlüsselt werden, mittels einer speziellen Spähsoftware („Staatstrojaner") vom Gerät des jeweiligen Nutzers auszuleiten und aufzuzeichnen.[15] Mit der Quellen-TKÜ wird „ein fremdes informationstechnisches System infiltriert, um mit einer eigens für diesen Zweck entwickelten Überwachungssoftware die Kommunikation zwischen den Beteiligten überwachen und aufzeichnen zu können".[16] In technischer Hinsicht erfolgt die Quellen-TKÜ daher nicht beim Telekommunikationsanbieter, sondern durch die Strafverfolgungsbehörden mittels Infiltration des jeweiligen informationstechnischen Systems.[17]

Die TKÜ erlaubt daher einen Eingriff in das Fernmeldegeheimnis des Art. 10 GG, während die Quellen-TKÜ *zusätzlich* das IT-Grundrecht betrifft.[18] Wegen dieser intensiveren Grundrechtsintensität ist die Quellen-TKÜ ggü. der TKÜ subsidiär, § 100a Abs. 1 S. 2 StPO a.E.[19] Verfassungsrechtlich gewendet wäre eine Quellen-TKÜ nicht erforderlich und daher unverhältnismäßig, wenn auch die unverschlüsselte Kommunikation des Beschuldigten überwacht werden kann.[20]

Beispielhaft liegt eine Quellen-TKÜ also dann vor, wenn Audiosignale eines laufenden Telekommunikationsvorgangs an einem Mikrofon überwacht werden.[21]

---

[12] BT-Drs. 18/12785, S. 46; siehe auch *Großmann*, JA 2019, 241 (243).

[13] BT-Drs. 18/12785, S. 48. Siehe auch *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100a Rn. 14a; *Großmann*, GA 2018, 439; *Ostendorf/Brüning*, Strafprozessrecht, 5. Aufl. 2024, § 8 Rn. 59; *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 220. Lesenswert und ausf. zum Ganzen (auch zu den technischen Details) *Graf*, in: BeckOK StPO, Stand: 1.1.2025, § 100a Rn. 113 f.; *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 42.

[14] So *Großmann*, GA 2018, 439; siehe auch *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 90; *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 3; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100a Rn. 14a.

[15] BT-Drs. 18/12785, S. 49. Siehe den Wortlaut von § 100a Abs. 1 S. 2 StPO: „[…] mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird […]." Zum Ganzen auch *Graf*, in: BeckOK StPO, Stand: 1.1.2025, § 100a Rn. 117 f.; *Krusel/Grzesiek*, KritV 2017, 331 (337); *Niedernhuber*, JA 2018, 169 (170); *Roggan*, StV 2017, 821 (822); *Volk/Engländer*, Grundkurs StPO, 10. Aufl. 2021, § 10 Rn. 40.

[16] BT-Drs. 18/12785, S. 46; siehe auch *Niedernhuber*, JA 2018, 169 (170).

[17] *Graf*, in: BeckOK StPO, Stand: 1.1.2025, § 100a Rn. 118.

[18] Siehe hierzu so explizit BVerfG NJW 2008, 822 (826); *Bantlin*, JuS 2019, 669 (671); siehe auch *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100a Rn. 9; *Graf*, in: BeckOK StPO, Stand: 1.1.2025, § 100a Rn. 117 f., 120; *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 3a; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100a Rn. 1. A.A. *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 91 f., 99, 120: Quellen-TKÜ greife nur in IT-Grundrecht ein.

[19] Siehe auch BVerfG NJW 2016, 1781 (1796 Rn. 234); BT-Drs. 18/12785, S. 51; *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 43; *Volk/Engländer*, Grundkurs StPO, 10. Aufl. 2021, § 10 Rn. 41; ausf. *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 218 f.

[20] Siehe auch *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 135.

[21] Siehe BT-Drs. 18/12785, S. 51.

b) Spezifika der Quellen-TKÜ

Die Quellen-TKÜ gem. § 100a Abs. 1 S. 2 StPO ist ein funktionelles Äquivalent zur TKÜ. Sie erlaubt daher *nicht* den Zugriff auf weitere Inhalte des informationstechnischen Systems, insbesondere dürfen keine Nachrichten ausgelesen werden, die *vor* der richterlichen Anordnung übermittelt oder empfangen wurden. Der Zugriff auf solche Informationen ist nur über § 100b StPO möglich.[22] Die Quellen-TKÜ gestattet folglich nur eine Überwachung der Telekommunikation, aber keine darüberhinausgehende umfassende Datenerhebung.[23] Der Begriff der *Überwachung* in § 100a StPO impliziert mit anderen Worten einen Bezug auf gegenwärtige, laufende Vorgänge.[24] So kann bspw. auf die noch unverschlüsselten Daten einer Telekommunikation via WhatsApp zurückgegriffen werden.[25] § 100a Abs. 1 S. 2 StPO legitimiert somit die Auslese *laufender* Kommunikation aus einem informationstechnischen System und soll somit den Eingriff in das Fernmeldegeheimnis des Art. 10 GG rechtfertigen.[26]

Auf bereits auf dem Endgerät des Betroffenen angekommene Kommunikationsdaten kann also mit § 100a Abs. 1 S. 2 StPO nicht zugegriffen werden.[27] Um diese Lücke zu schließen, erlaubt § 100a Abs. 1 S. 3 StPO *ergänzend* den Zugriff auf solche Kommunikationsdaten, deren Übertragungsvorgang bereits abgeschlossen ist, weshalb diese Vorschrift keine Grundlage für Eingriffe in Art. 10 GG enthält, sondern in das IT-Grundrecht.[28] Angesprochen sind insbesondere über Messenger-Dienste (WhatsApp etc.) versendete Nachrichten. Diese zweite Form der Quellen-TKÜ wird auch „kleine Online-Durchsuchung" genannt, weil sie sich – anders als § 100b StPO – nur auf Telekommunikationsdaten bezieht (§ 100a Abs. 1 S. 3 StPO) und dass auch nur hinsichtlich solcher Telekommunikation, die *nach* der Anordnung der Maßnahme erfolgt.[29]

In beiden Fällen liegt im Vergleich zur regulären TKÜ i.S.d. § 100a Abs. 1 S. 1 StPO ein zusätzlicher Eingriff dergestalt vor, dass eine Software in das informationstechnische System des Betroffenen eingeschleust wird.[30]

c) Anordnungsvoraussetzungen

Der Gesetzgeber betont zutreffend, dass die TKÜ einen schwerwiegenden Eingriff in das durch Art. 10 Abs. 1 GG geschützte Fernmeldegeheimnis darstellt und somit unter einem besonderen Rechtfertigungsdruck steht.[31] Erforderlich für die verfassungsrechtliche Rechtfertigung dieses Eingriffs ist pri-

---

[22] BT-Drs. 18/12785, S. 50.

[23] Ausf. *Grözinger*, GA 2019, 441 (445 ff., 451).

[24] *Grözinger*, GA 2019, 441 (445 f.).

[25] *Volk/Engländer*, Grundkurs StPO, 10. Aufl. 2021, § 10 Rn. 40.

[26] *Beulke/Swoboda*, Strafprozessrecht, 16. Aufl. 2022, Rn. 393; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100a Rn. 1, 14a ff.; *Niedernhuber*, JA 2018, 169 (170 f.).

[27] Siehe *Graf*, in: BeckOK StPO, Stand: 1.1.2025, § 100a Rn. 116, 122; *Großmann*, JA 2019, 241 (243).

[28] *Großmann*, JA 2019, 241 (243); *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 140 ff., 146; *Niedernhuber*, JA 2018, 169 (170 f.).

[29] *Sinn*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Strafgesetzbuchs, des Jugendgerichtsgesetzes, der Strafprozessordnung und weiterer Gesetze BT-Drs. 18/11272, S. 5; *Krusel/Grzesiek*, KritV 2017, 331 (335 f.). Entscheidend ist also der Zeitpunkt der Anordnung, nicht derjenige der Installation der Spähsoftware. Das stellt auch § 100a Abs. 5 S. 1 Nr. 1 lit. b StPO klar. Zum Ganzen *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 44; *Großmann*, JA 2019, 241 (243); *Grözinger*, GA 2019, 441 (444 f.); *Niedernhuber*, JA 2018, 169 (171); *Ostendorf/Brüning*, Strafprozessrecht, 5. Aufl. 2024, § 8 Rn. 59.

[30] BT-Drs. 18/12785, S. 51; siehe auch *Roggan*, StV 2017, 821. Technische Details gibt bspw. *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100b Rn. 14.

[31] BT-Drs. 19/14747, S. 28; siehe auch *Bruns*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 1; *Roggan*, StV 2017, 821.

mär, dass die Maßnahme nur zur Aufklärung einer *schweren* Straftat eingesetzt wird, § 100a Abs. 1 S. 1 Nr. 1 StPO i.V.m. § 100a Abs. 2 StPO. Das BVerfG gesteht dem Gesetzgeber auch insofern eine Einschätzungsprärogative für die Entscheidung zu, „welche Straftaten er zum Anlass für bestimmte strafprozessuale Ermittlungsmaßnahmen machen möchte".[32] Für die konkrete Anordnung ist erforderlich, dass „bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer" eine der Katalogtaten begangen hat, § 110a Abs. 1 S. 1 Nr. 1 StPO. Sachlich ist damit ein qualifizierter Anfangsverdacht gemeint.[33] Notwendig hierfür ist eine konkrete Tatsachenbasis, ein hinreichender oder gar dringender Tatverdacht wird jedoch nicht vorausgesetzt.[34]

Die Telekommunikationsüberwachung darf unter folgenden Voraussetzungen angeordnet werden:

- Es muss der begründete Verdacht bestehen, dass jemand an einer schweren Straftat i.S.d. § 100a Abs. 2 StPO beteiligt war.
- Diese Tat muss auch im Einzelfall schwer wiegen. Die bloß abstrakte Schwere der Tat genügt nicht, § 100a Abs. 1 S. 2 Nr. 2 StPO.[35]
- Die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten muss ohne die Überwachung der Telekommunikation wesentlich erschwert oder aussichtslos sein, § 100a Abs. 1 S. 2 Nr. 3 StPO (Subsidiaritätsklausel).[36]
- Der Kreis möglicher Betroffener der Maßnahme wird von § 100a Abs. 3 StPO gezogen.
- Die Anordnungskompetenz richtet sich nach § 100e Abs. 1 S. 1 StPO. Im Ermittlungsverfahren ist also grundsätzlich der Ermittlungsrichter zuständig, § 162 Abs. 1 StPO.

Während § 100a Abs. 1 S. 2 Nr. 1 StPO also eine abstrakte Voraussetzung statuiert, machen Nr. 2 und 3 eine Einzelfallprüfung erforderlich. Die Tat muss mit anderen Worten auch im konkreten Einzelfall schwer wiegen. Der Gesetzgeber verweist bspw. auf die Möglichkeit, dass durch einen Wohnungseinbruchdiebstahl im Einzelfall die Privatsphäre des Geschädigten „nicht intensiv beeinträchtigt wurde", sodass der konkrete Schuldgehalt der Tat nicht i.S.d. § 100a Abs. 1 S. 2 Nr. 1 StPO schwer genug wiegt. Im Falle einer serienmäßigen Begehung könne hingegen eine konkrete Schwere der Tat begründen.[37]

Ein entsprechender Regelungsmechanismus ist bei der Online-Durchsuchung und der akustischen Wohnraumuntersuchung vorgesehen, §§ 100b Abs. 1 Nr. 2, 100c Abs. 1 Nr. 2 StPO. In der Begründung der Anordnung ist dieser Eingriffsgrenze einzelfallbezogen zu entsprechen, um so die Verhältnismäßigkeit der Maßnahme sicherzustellen, siehe § 100e Abs. 4 S. 2 StPO.[38]

In formeller Hinsicht sind die Protokollierungspflichten gem. § 100a Abs. 6 StPO zu beachten. Die entsprechenden Angaben sollen eine nachträgliche richterliche Überprüfung der Maßnahme ermög-

[32] BVerfG NJW 2012, 833 (836).

[33] *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100a Rn. 30; *Großmann*, JA 2019, 241 (242).

[34] Zu den Einzelheiten siehe *Soiné*, NStZ 2018, 497 (498); ausf. *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100a Rn. 151 ff.

[35] Siehe auch BT-Drs. 19/14747, S. 29.

[36] Die Subsidiaritätsklausel dient der Umsetzung des Erfordernisses der Erforderlichkeit als Teil des Verhältnismäßigkeitsprinzips, siehe *Krey/Heinrich*, Deutsches Strafverfahrensrecht, 2. Aufl. 2018, Rn. 880.

[37] BT-Drs. 19/14747, S. 29.

[38] Ausf. zu dieser qualifizierten Begründungspflicht *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100e Rn. 52 ff.

lichen.[39] Aus Sicht der Rechtspflege geht es spiegelbildlich um die „Gerichtsfestigkeit" der erhobenen Informationen.[40]

2. Die akustische Wohnraumüberwachung gem. § 100c StPO

§ 100c StPO regelt den sog. großen Lauschangriff.[41] § 100c StPO erlaubt die Abhörung und Aufzeichnung des in einer Wohnung nicht öffentlich gesprochenen Wortes. Damit ist § 100c StPO eine Eingriffsgrundlage in das Grundrecht auf Unverletzlichkeit der Wohnung gem. Art. 13 GG.[42] Wegen der vom BVerfG betonten Nähe von Eingriffen in das IT-Grundrecht einerseits und einer akustischen Wohnraumüberwachung sind die Voraussetzungen des § 100c StPO im Wesentlichen parallel zu denjenigen der Online-Durchsuchung, insbesondere muss eine entsprechende Katalogtat vorliegen, § 100c Abs. 1 Nr. 1 StPO. In technischer Hinsicht wird die Wohnraumüberwachung durch Richtmikrofone, aber auch mittels kleiner batteriebetriebenen Minisendern, den sog. Wanzen, realisiert.[43]

3. Die Online-Durchsuchung gem. § 100b StPO

a) Grundlegung

Die Online-Durchsuchung wurde 2017 mit dem Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens in die StPO eingeführt.[44] § 100b StPO betrifft keine Datenerhebungen *während* einer laufenden Kommunikation und legitimiere somit Eingriffe in das IT-Grundrecht.[45] Der Begriff des informationstechnischen Systems i.S.d. § 100b StPO hat daher entsprechend des Schutzbereichs des IT-Grundrechts zu erfolgen.[46] Das hat insbesondere zur Folge, dass das informationstechnische System nicht kommunikationsbezogen (i.S.d. § 100a StPO) auszulegen ist.[47]

Als Online-Durchsuchung „wird der verdeckte staatliche Zugriff auf fremde informationstechnische Systeme über Kommunikationsnetze mittels einer Überwachungssoftware bezeichnet."[48] Die Online-Durchsuchung legitimiert den verdeckten Zugriff auf ein informationstechnisches System mittels Infiltrierung von Spähsoftware, betrifft sämtliche Daten, die in diesem System gespeichert

---

[39] *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 163.

[40] BT-Drs. 18/12785, S. 53.

[41] Siehe hierzu bspw. BVerfGE 109, 279; *Gercke*, GA 2015, 339; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100c Rn. 2; *Krey/Heinrich*, Deutsches Strafverfahrensrecht, 2. Aufl. 2018, Rn. 889. Der kleine Lauschangriff betrifft demgegenüber das außerhalb der Wohnung gesprochene nicht öffentliche Wort. Dieser richtet sich nach § 100f StPO, siehe zum Ganzen nur *Beulke/Swoboda*, Strafprozessrecht, 16. Aufl. 2022, Rn. 414. Ausf. zum Verhältnis von Lauschangriff und Grundgesetz *Gusy*, JuS 2004, 457. Zur rechtspolitischen Diskussion *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 42.

[42] BT-Drs. 18/12785, S. 48; *Volk/Engländer*, Grundkurs StPO, 10. Aufl. 2021, § 10 Rn. 51; *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100c Rn. 2. Siehe auch BVerfG NJW 2016, 1781 (1792 Rn. 179).

[43] Siehe hierzu *Blechschmitt*, MMR 2018, 361 (365); *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100c Rn. 85.

[44] BGBl. I 2017, S. 3202. Zur Rechtslage bis zu dieser Reform siehe *Ruhmannseder*, JA 2009, 57 (61).

[45] BT-Drs. 18/12785, S. 54; *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100b Rn. 1 f., 6; *Heinrich*, ZIS 2020, 421; *Grözinger*, GA 2019, 441 (444); *ders.*, StV 2009, 406; *Roggan*, StV 2017, 821 (827).

[46] *Grözinger*, StV 2009, 406 (411); *Niedernhuber*, JA 2018, 169 (171).

[47] Siehe *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100b Rn. 98.

[48] BT-Drs. 18/12785, S. 46; siehe auch *Singelnstein/Derin*, NJW 2017, 2646 f.

sind und bedeutet gerade deswegen einen schwerwiegenden Eingriff in die Privatsphäre des Betroffenen.[49]

b) Abgrenzung zur Quellen-TKÜ

§ 100b StPO legitimiert eine heimliche, auf Dauer angelegte Ausspähung des Betroffenen.[50] Der mit der Online-Durchsuchung verbundene Eingriff ist eine verdeckte Maßnahme, die in ihrem Umfang erheblich weiter reicht als Eingriffe nach § 100a StPO.[51]

§ 100b StPO erfasst in Abgrenzung zur Quellen-TKÜ auch die Auslese von Kommunikationsinhalten, die *vor* einer richterlichen Anordnung einer Maßnahme nach § 100a StPO erfolgt ist.[52] Damit unterscheidet sich die Online-Untersuchung von der Quellen-TKÜ nicht durch technische Details,[53] sondern durch das Ausmaß und den Umfang der Daten, die gem. § 100b StPO ausgeleitet werden dürfen.[54] Weil informationstechnische Systeme so eine überragende Rolle im modernen Leben der Menschen spielt, können die Strafverfolgungsbehörden auf einen schier unermesslichen Datenschatz zugreifen, der berufliche, private und höchstpersönliche Informationen in Form von Nachrichten, Kontaktdaten, Fotos, GPS-Daten etc. umfasst.[55] Die Kategorisierung als „digitale Allzweckwaffe“[56] ist daher durchaus treffend.

Dementsprechend wiegt die Onlinedurchsuchung auch schwerer als eine offene Beschlagnahme gem. §§ 94 ff., 102 ff. StPO der informationstechnischen Geräte mit anschließender Auslese. Weil das BVerfG klargestellt hatte, dass eine Online-Durchsuchung ihrer Eingriffsintensität nach mit einer akustischen Wohnraumüberwachung vergleichbar ist,[57] hat sich der Gesetzgeber für die Ausgestaltung des 100b StPO an vor 2017 geltenden Fassung des § 100c StPO orientiert.[58] Das lässt sich mit guten Gründen kritisieren. Während nämlich § 100c StPO die Abhörung und Aufzeichnung des „nicht öffentlich gesprochenen Wortes“ erlaubt, eröffnet § 100b StPO Zugriff auf eine schier endlose Datenmenge, seien es Fotos, Nachrichten und Kontaktdaten, Kalendereinträge, Suchmaschinendaten oder Notizen – sodass § 100b StPO ggf. auch Informationen erfasst, die der Betroffene noch nicht einmal aussprechen würde, weshalb die Eingriffsintensität von § 100b StPO im Hinblick auf die Privatsphäre sehr viel umfangreicher ist als diejenige der akustischen Wohnraumüberwachung.[59]

§ 100b Abs. 1 StPO legitimiert eine Datenerhebung nur *aus* dem infiltrierten System. Erlaubt ist also nur eine *passive* Kenntnisnahme. Darüberhinausgehende Tätigkeiten wie die Aktivierung des Mikrofons oder der Kamera eines Smartphones zu entsprechenden Überwachungsmaßnahmen sind

[49] *Großmann*, GA 2018, 439 (440); *Köhler*, in: Meyer-Goßner/Schmitt, Strafprozessordnung mit GVG und Nebengesetzen, Kommentar, 67. Aufl. 2024, § 100a Rn. 1.

[50] Dem ist sich der Gesetzgeber wohl bewusst, siehe BT-Drs. 18/12785, S. 54.

[51] *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100a Rn. 9.

[52] BT-Drs. 18/12785, S. 53.

[53] Klarstellend *Krusel/Grzesiek*, KritV 2017, 331 (336 f.); *Hauck*, in: Löwe/Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Bd. 3/1, 27. Aufl. 2019, StPO § 100a Rn. 93: Quellen-TKÜ und Online-Durchsuchung erfordern in technischer Hinsicht Infiltration des informationstechnischen Systems.

[54] *Roggan*, StV 2017, 821 (825).

[55] *Soiné*, NStZ 2018, 497 (502).

[56] So *Krusel/Grzesiek*, KritV 2017, 331.

[57] Siehe BVerfG NJW 2016, 1781 (1784 Rn. 108).

[58] BT-Drs. 18/12785, S. 54; siehe auch *Großmann*, GA 2018, 439 (441 f.).

[59] Zutreffend *Großmann*, GA 2018, 439 (445 f.); siehe auch *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100b Rn. 2 f.

nach verbreiteter Ansicht nicht gedeckt.[60] Wurde das Mikrofon jedoch vom Betroffenen aktiviert, können aus dem infiltrierten System entsprechende Daten erhoben werden.[61]

Wurden über das vom Nutzer aktivierte Mikrophon zudem Gespräche in der Wohnung des Betroffenen aufgenommen, ist umstritten, ob diese nur verwertet werden, wenn auch eine Anordnung nach § 100c StPO vorlag.[62] Insofern dürfte das Verfassungsrecht die maßgeblichen Argumente liefern: Das Gesetz, mit dem § 100b StPO eingeführt wurde, zitiert i.S.d. Art. 19 Abs. 1 S. 2 GG als von der Online-Durchsuchung eingeschränktes Grundrecht nicht Art. 13 GG, weswegen die Online-Durchsuchung Eingriffe in dieses Grundrecht nicht zu legitimieren vermag.[63] Deswegen erlaubt § 100b StPO auch nicht (als Annexkompetenz) die Betretung der Wohnung des Betroffenen, um so die Spähsoftware zu installieren.[64]

c) Verfassungsrechtliche Bezüge und einige kritische Anmerkungen

Die von § 100b StPO vorgesehenen massiven Eingriffe in das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme bedürfen einer besonderen Ermächtigung.[65] Das BVerfG vergleicht die Eingriffsintensität einer Online-Durchsuchung mit derjenigen einer akustischen Wohnraumüberwachung.[66] Im Gefahrenabwehrrecht hat das Gericht daher klargestellt, dass der entsprechende Eingriff nur gerechtfertigt sein kann, wenn „tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen".[67] Für den Bereich der Strafverfolgung deutet der Gesetzgeber diese Vorgaben so, dass sich der Tatverdacht auf eine Straftat beziehen muss, deren Schwere und Bedeutung in einem angemessenen Verhältnis zur Eingriffsschwere der Online-Durchsuchung steht.[68]

Hieraus ergibt sich also ein offenkundiger Unterschied zwischen den Regelungen der §§ 100a und 100b StPO. Während die (Quellen-)TKÜ beim Verdacht einer *schweren* Straftat gestattet ist, setzt die Onlinedurchsuchung den Verdacht einer *besonders schweren* Straftat voraus (§§ 100a Abs. 1 S. 1 Nr. 1, 100b Abs. 1 Nr. 1 StPO). Diese Differenzierung dient letztlich der Sicherstellung der Verhältnismäßigkeit der jeweiligen Maßnahme und folgt Vorgaben des BVerfG.[69] Wegen der vom BVerfG gezogenen Parallele sind die Katalogtaten der akustischen Wohnraumüberwachung und der Online-Durchsuchung identisch, siehe § 100c Abs. 1 Nr. 1 StPO.[70] Aus diesem Regelungszusammenhang folgt, dass die Begriffe der schweren Straftat und der besonders schweren Straftat nicht identisch gebraucht werden dürfen.[71] Eine besonders schwere Straftat übersteigt den mittleren Kriminalitätsbereich deutlich.[72]

---

[60] *Roggan*, StV 2017, 821 (826); *Großmann*, GA 2018, 439 (442); *Singelnstein/Derin*, NJW 2017, 2646 (2647); *Soiné*, NStZ 2018, 497 (502). Siehe auch *Blechschmitt*, MMR 2018, 361 (365). Krit. *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100b Rn. 5.

[61] Siehe *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100b Rn. 44 ff.; *Blechschmitt*, MMR 2018, 361 (365).

[62] Bejahend *Soiné*, NStZ 2018, 497 (503 f.); krit. *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 100b Rn. 47 f.

[63] Siehe Art. 17 des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens v. 17.8.2017, BGBl. I 2017, S. 3202, 3213. Zum Ganzen auch *Roggan*, StV 2017, 821 (826).

[64] *Bär*, in: KMR-StPO, 133. Lfg., Stand: 1.12.2024, § 100b Rn. 13; *Soiné*, NStZ 2018, 497 (501).

[65] Zu den Anordnungsvoraussetzungen siehe *Soiné*, NStZ 2018, 497 (498 ff.).

[66] BVerfG NJW 2016, 1781 (1794 Rn. 210 a.E.).

[67] BVerfG NJW 2008, 822; BVerfG NJW 2016, 1781 (1795 Rn. 212).

[68] BT-Drs. 18/12785, S. 54.

[69] Siehe BVerfGE 107, 299 (322); 109, 279 (346); 113, 348 (388); siehe auch *Ruhmannseder*, JA 2009, 57 (58).

[70] BT-Drs. 18/12785, S. 54. Siehe auch *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100b Rn. 10.

[71] Ausf. hierzu *Rieß*, GA 2004, 623 ff.; *Krusel/Grzesiek*, KritV 2017, 331 (346).

[72] *Henrichs/Weingast*, in: KK-StPO, 9. Aufl. 2023, § 100c Rn. 9.

Die insofern verwendete Terminologie muss jedoch verwirren und begründet in Folge dessen eine Kritik an der Reichweite des § 100b StPO. Der Sprung zur allgemeinen Kategorisierung der Straftaten in § 12 Abs. 1, Abs. 2 StGB ist wahrlich nicht weit und es leuchtet ad hoc sehr ein, von besonders schweren Straftaten nur dann zu sprechen, wenn es sich um *Verbrechen* im Sinne des materiellen Strafrechts handelt. Diesen Weg ist der Gesetzgeber jedoch nicht gegangen, vielmehr finden sich unter den Katalogtaten des § 100b Abs. 2 StPO diverse Vergehen, wie bspw. §§ 89a StGB, 89c, 184b Abs. 2 StGB, § 84 Abs. 3 AsylG, § 96 Abs. 2 AufenthG.[73] Der Eindruck der Kritisierbarkeit des § 100b StPO verstärkt sich noch, wenn man berücksichtigt, dass das BVerfG betont, dass Eingriffe in das IT-Grundecht nur zum Schutz überragend wichtiger Rechtsgüter zulässig sind.[74] Das BVerfG nennt in diesem Zusammenhang „Leib, Leben und Freiheit der Person sowie solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt".[75] Unter diesen Gesichtspunkten ist es durchaus bemerkenswert, dass auch Tatbestände aus dem BtMG (§ 100b Abs. 2 Nr. 5 StPO), dem WaffG (§ 100b Abs. 2 Nr. 10 StPO) oder dem AsylG (§ 100b Abs. 2 Nr. 2 StPO) zu den Katalogtaten gezählt werden, Delikte zum Schutz der Umwelt hingegen nicht.[76] § 100b StPO bietet also sehr weitreichende Ermittlungsbefugnisse für einen umfangreichen Katalog von Straftaten. Zweifel an der Verfassungsmäßigkeit des § 100b StPO wurden deswegen erhoben.[77] Für die Rechtmäßigkeit der konkreten Anordnung ist vor allem die Subsidiaritätsklausel des § 100b Abs. 1 Nr. 3 StPO wichtig, die sicherstellen soll, dass die Maßnahme nur in den *erforderlichen* Fällen erfolgt.[78]

4. Gemeinsame Verfahrensvorschriften

Das für die Maßnahmen nach §§ 100a–100c StPO wesentlichen Verfahrensvorschriften sind nach geltender Rechtslage komprimiert in § 100e StPO geregelt. Die Vorschrift soll nach Auffassung des Gesetzgebers jedoch gestufte Voraussetzungen für die divergierende Eingriffsintensität der einzelnen Maßnahmen vorsehen.[79]

Maßnahmen nach § 100a StPO dürfen grundsätzlich nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden, bei Gefahr im Verzug darf die Staatsanwaltschaft die Maßnahme anordnen, § 100e Abs. 1 S. 1, 2 StPO. Die Zuständigkeit richtet sich nach allgemeinen Regeln, im Ermittlungsverfahren ist also der Ermittlungsrichter zuständig, § 162 Abs. 1 StPO. Die Maßnahme darf grundsätzlich nur für eine Dauer von drei Monaten angeordnet werden, § 100e Abs. 1 S. 4 StPO.

Die Anordnung der Maßnahmen nach §§ 100b, 100c StPO erfolgt grundsätzlich gem. § 100d Abs. 2 StPO auf Antrag der Staatsanwaltschaft durch eine mit drei Richtern besetzte Kammer des Landgerichts i.S.d. § 74a Abs. 4 GVG. Bei Gefahr im Verzug entscheidet der Vorsitzende dieser Kammer, nicht die Staatsanwaltschaft. Die Maßnahme darf grundsätzlich nur für eine Dauer von einem Monat

[73] Krit. daher *Roxin/Schünemann*, Strafverfahrensrecht, 30. Aufl. 2022, § 36 Rn. 6.
[74] BVerfG NJW 2008, 822.
[75] BVerfG NJW 2008, 822 (831 Rn. 247).
[76] Siehe auch *Grözinger*, StV 2009, 406 (411 f.).
[77] *Grözinger*, Die Überwachung von Cloud Storage, 2018, S. 304 ff.; *Großmann*, JA 2019, 241 (244); siehe auch *ders.*, GA 2018, 439; *Krusel/Grzesiek*, KritV 2017, 331 (344 ff.); *Roggan*, StV 2017, 821 (826); *Singelstein/Derin*, NJW 2017, 2646 (2647). Derzeit sind mehrere Verfassungsbeschwerden beim BVerfG anhängig (Az. 1 BvR 180/23), mit denen die Verfassungswidrigkeit insbesondere der §§ 100a Abs. 1 S. 2, 100b StPO gerügt wird.
[78] Hierzu *Soiné*, NStZ 2018, 497 (499).
[79] BT-Drs. 18/12785, S. 57.

angeordnet werden, § 100e Abs. 2 S. 4 StPO. Verstöße gegen diese Kompetenzvorschriften ziehen richtigerweise ein Beweisverwertungsverbot nach sich.[80]

§ 100e StPO Abs. 3 StPO enthält dezidierte Vorgaben über den Inhalt der Entscheidungsformel der Anordnung, Abs. 4 regelt den notwendigen Inhalt der Begründung der Anordnung. Die Anordnung muss namentlich die wesentlichen Gesichtspunkte der Abwägung zwischen der Bedeutung des Ermittlungsverfahrens und der beeinträchtigten Grundrechte enthalten, § 100e Abs. 4 S. 1 StPO. Zudem sind die relevanten Daten, die erhoben werden sollen, bereits so präzise wie möglich zu bezeichnen, § 100e Abs. 3 Nrn. 3 und 4 StPO).

5. Richtervorbehalt und nachträglicher Rechtsschutz

Mit der Eröffnung der Möglichkeit des Rechtsschutzes gem. Art. 19 Abs. 4 GG ist für den vorliegenden Bereich eine weitere wichtige verfassungsrechtliche Regelung angesprochen.[81] Dass der Bürger gegen hoheitliche Maßnahmen, von denen er betroffen ist, Rechtsschutz suchen kann, ist eine wesentliche Ausprägung des Rechtsstaatsprinzips.[82] Bzgl. des Rechtsschutzes gegen Zwangsmittel differenziert die StPO zwischen offenen und verdeckten bzw. geheimen Maßnahmen.[83] Wie die unterschiedlichen Regelungen in Art. 13 Abs. 2 GG einerseits und Art. 13 Abs. 3, Abs. 4 GG andererseits belegen, wiegen geheime Überwachungsmaßnahmen vor den Toren des Grundgesetzes schwerer als offene Maßnahmen.[84]

Definitionsgemäß ist bei den verdeckten Maßnahmen der §§ 100a ff. StPO individueller Rechtsschutz nur sehr eingeschränkt möglich.[85] Die Eingriffsintensität der verdeckten Maßnahmen sind im Verbund mit der sachlich ausgeschlossenen Möglichkeit präventiven gerichtlichen Rechtsschutzes gravierende Argumente für den (grundsätzlichen) Richtervorbehalt bei der Anordnung der Maßnahmen nach §§ 100a ff. StPO: Gerade weil Art. 19 Abs. 4 S. 1 GG effektiven Rechtsschutz garantiert, dieser im Falle verdeckter Maßnahmen vom Betroffenen aber erst nachträglich angestrengt werden kann, ist es verfassungsrechtlich geboten, Gerichte schon im Anordnungsstadium zu beteiligen.[86] Der Richtervorbehalt installiert eine unabhängige und objektive Kontrollinstanz vor der entsprechenden grundrechtsbeeinträchtigenden Maßnahme, die das Grundrecht zusätzlich absichern soll.[87]

Im Übrigen erkennt der Gesetzgeber die gehobene Bedeutung eines effektiven *repressiven* Rechtsschutzes an.[88] Um diesen zu ermöglichen, sehen die einzelnen Vorschriften insbesondere Dokumentationspflichten vor, siehe §§ 100a Abs. 6, 100b Abs. 4, 101 Abs. 2 StPO.[89] Außerdem sind die Betroffenen von den Maßnahmen *grundsätzlich*[90] zu benachrichtigen, „sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a StPO auch der Möglichkeit

[80] *Großmann*, JA 2019, 241 (247); für die Online-Durchsuchung *Soiné*, NStZ 2018, 497 (504).
[81] Siehe BVerfG NJW 1997, 2163; BVerfG NJW 2012, 833 (834 f.); *Zeyher*, JuS 2022, 636; *Zöller*, ZStW 124 (2012), 411 (434); allg. zum Ganzen auch *Glaser*, JR 2010, 423 ff., *Singelnstein*, NStZ 2009, 481.
[82] Siehe hierzu *Hufen*, Verwaltungsprozessrecht, 13. Aufl. 2024, § 1 Rn. 5.
[83] Siehe hierzu ausf. *Burghardt*, JuS 2010, 605; *Meyer/Rettenmaier*, NJW 2009, 1238; siehe auch *Zeyher*, JuS 2022, 636 (637 f.).
[84] Klarstellend *Michael/Morlok*, Grundrechte, 9. Aufl. 2025, Rn. 669.
[85] Siehe *Roggan*, StV 2017, 821 (826).
[86] *Hilger*, JR 1990, 485. Siehe auch *Kindhäuser/Schumann*, Strafprozessrecht, 7. Aufl. 2023, § 8 Rn. 76.
[87] *Michael/Morlok*, Grundrechte, 9. Aufl. 2025, Rn. 592; *Zöller*, ZStW 124 (2012), 411 (428 f.).
[88] BT-Drs. 18/12785, S. 47.
[89] Siehe hierzu *Hegmann*, in: BeckOK StPO, Stand: 1.1.2025, § 101 Rn. 50.
[90] Zu den Ausnahmen siehe § 101 Abs. 4 S. 2 und 3 StPO.

der weiteren Verwendung des Verdeckten Ermittlers möglich ist", § 101 Abs. 4 S. 1, Abs. 5 S. 1 StPO. Mit der Benachrichtigung ist auf die Möglichkeit nachträglichen Rechtsschutzes hinzuweisen, § 101 Abs. 4 S. 2 StPO. Innerhalb von zwei Wochen nach dieser Benachrichtigung können die Betroffenen auch nach Beendigung der Maßnahme die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen, § 101 Abs. 7 S. 2 StPO.[91]

Gleichwohl sind unter dem Gesichtspunkt des effektiven Rechtsschutzes verdeckte Maßnahmen verfassungsrechtlich problematisch und sollen nach der Rechtsprechung des BVerfG eine begründungsbedürftige Ausnahme darstellen.[92]

[91] Siehe *Burghardt*, JuS 2010, 605 (607). Ausf. hierzu *Rückert*, in: MüKo-StPO, Bd. 1, 2. Aufl. 2023, § 101 Rn. 87 ff.
[92] BVerfG NJW 2009, 2431.