



Sachstand

Behördlicher Einsatz sogenannter „Spähsoftware“ Rechtliche Rahmenbedingungen

Behördlicher Einsatz sogenannter „Spähsoftware“

Rechtliche Rahmenbedingungen

Aktenzeichen:	WD 7 - 3000 - 067/24; WD 3 - 3000 - 102/24
Abschluss der Arbeit:	08.10.2024 (zugleich letzter Abruf der Links)
Fachbereiche:	WD 7: Zivil-, Straf- und Verfahrensrecht, Medienrecht, Bau und Stadtentwicklung (Gliederungspunkte 1 und 2) WD 3: Verfassung und Verwaltung (Gliederungspunkte 1 und 3)

Die Wissenschaftlichen Dienste des Deutschen Bundestages unterstützen die Mitglieder des Deutschen Bundestages bei ihrer mandatsbezogenen Tätigkeit. Ihre Arbeiten geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Arbeiten der Wissenschaftlichen Dienste geben nur den zum Zeitpunkt der Erstellung des Textes aktuellen Stand wieder und stellen eine individuelle Auftragsarbeit für einen Abgeordneten des Bundestages dar. Die Arbeiten können der Geheimschutzordnung des Bundestages unterliegende, geschützte oder andere nicht zur Veröffentlichung geeignete Informationen enthalten. Eine beabsichtigte Weitergabe oder Veröffentlichung ist vorab dem jeweiligen Fachbereich anzuzeigen und nur mit Angabe der Quelle zulässig. Der Fachbereich berät über die dabei zu berücksichtigenden Fragen.

Inhaltsverzeichnis

1.	Einleitung	4
2.	Strafverfolgung	4
2.1.	Quellen-Telekommunikationsüberwachung	4
2.2.	Online-Durchsuchung	6
2.3.	Zuständigkeit und Verfahren	8
3.	Gefahrenabwehr	9
3.1.	Bundespolizei	9
3.2.	Zollkriminalamt	9
3.3.	Nachrichtendienste	10
3.4.	Bundeskriminalamt	11
3.5.	Berührte Grundrechte und Kontrolle	12

1. Einleitung

Die deutsche Rechtsordnung unterscheidet in Bezug auf den Einsatz sogenannter **Spähsoftware**¹ zwischen der **Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)** und der **Online-Durchsuchung**. Das Instrument der Quellen-TKÜ steht bei Vorliegen der gesetzlichen Voraussetzungen im Einzelfall den Nachrichtendiensten des Bundes, dem Bundeskriminalamt (BKA), dem Zollkriminalamt sowie den Strafverfolgungsbehörden im Ermittlungsverfahren zur Verfügung. Letztere sind auch zur Durchführung von Online-Durchsuchungen berechtigt. Gleiches gilt für das BKA auch zum Zwecke der Abwehr von Gefahren des internationalen Terrorismus. Zu nachrichtendienstlichen Zwecken darf die Online-Durchsuchung nur in sehr beschränktem Maße eingesetzt werden.

2. Strafverfolgung

Im Rahmen der Strafverfolgung ist es den zuständigen Behörden in bestimmten Fällen gestattet, Spähsoftware auf den informationstechnischen Systemen des mutmaßlichen Täters zu installieren und zu nutzen. Unerheblich ist insofern, ob es sich um Bundes- oder Landesbehörden handelt und welche Strafverfolgungsbehörde im Einzelnen agiert. Die einschlägigen Regelungen gelten mithin sowohl für den **Regelfall einer ermittelnden lokalen Staatsanwaltschaft** (als Landesbehörde) wie etwa auch für das **Bundeskriminalamt**.²

2.1. Quellen-Telekommunikationsüberwachung

Gemäß § 100a Absatz 1 Satz 2 StPO³ darf die **Überwachung und Aufzeichnung von Telekommunikation** zum Zweck der Strafverfolgung in der Weise erfolgen, dass mit **technischen Mitteln** in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Hierbei handelt es sich um die **Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)**. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen dabei gemäß § 100a Absatz 1 Satz 3 StPO überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können. Bei der Quellen-TKÜ müssen stets auch die Voraussetzungen der normalen

1 Alternativ sind u.a. auch die Bezeichnungen „Spionagesoftware“, „Staatstrojaner“ oder auch „Bundestrojaner“ gebräuchlich, vgl. Heckmann/Paschke, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Auflage 2022, § 121 Rn. 86 m.w.N.; Großmann, Telekommunikationsüberwachung und Online-Durchsuchung: Voraussetzungen und Beweisverbote, JA 2019, 241, 243; Graf, in: BeckOK StPO, 52. Edition, Stand: 1.4.2024, § 100a Rn. 113 f.; Werner, in: Weber, Rechtswörterbuch, 33. Edition 2024, Stichwort Staatstrojaner.

2 Vgl. zum BKA https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/Quellentkue-Online-durchsuchung/quellentkue-Online-durchsuchung_node.html.

3 Strafprozeßordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 3 des Gesetzes vom 30.07.2024 (BGBl. 2024 I Nr. 255) geändert worden ist.

Telekommunikationsüberwachung vorliegen.⁴ Unter den Begriff der technischen Mittel wird auch Spähsoftware subsumiert:

„Der Begriff des technischen Mittels ist weit gefasst. Hierunter lassen sich verschiedene technische Methoden subsumieren, mittels derer die Erhebung von Telekommunikationsdaten von einem informationstechnischen System möglich sind. Nach derzeitigem Stand der Technik umfasst dies vor allem Spähsoftware (sog. Staatstrojaner) mit unterschiedlichen Funktionsweisen (zB der Möglichkeit, Daten vom System zu kopieren, lokal zu speichern und an einen Command-and-Control-Server der Behörden auszuleiten, Screenshots vom Bildschirm des Geräts anzufertigen, Zugriff auf verschiedene Funktionalitäten des Systems zu nehmen etc) aber auch Hardwarelösungen wie zB Hardware-Keylogger, welche die Tastaturanschläge und/oder Mausklicks protokollieren und speichern.“⁵

Eine Quellen-TKÜ darf stets nur erfolgen, „wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen“ (§ 100a Absatz 1 Satz 2 StPO). Sie betrifft demnach vor allem den verschlüsselten Datenverkehr, der von einer herkömmlichen TKÜ im Sinne von § 100a Absatz 1 Satz 1 StPO nur aufgrund der Verschlüsselung nicht erfasst werden kann, und ist subsidiär zur TKÜ.⁶

Die Vorschrift unterscheidet zwischen der Überwachung und Aufzeichnung **laufender** Telekommunikation (§ 100a Absatz 1 Satz 2 StPO) und **gespeicherten** Kommunikationsinhalten und -umständen (§ 100a Absatz 1 Satz 3 StPO). Beide Varianten setzen einen Eingriff mit technischen Mitteln voraus, womit der Zugriff auf das IT-System durch eine entsprechende Software gemeint ist.⁷

Bei der Überwachung und Aufzeichnung der in einer Anwendung gespeicherten Kommunikationsinhalte und -umstände einer abgeschlossenen Übertragung nach § 100a Absatz 1 Satz 3 StPO dürfen **keine anderweitigen Daten** des Endgeräts, die unabhängig von der Kommunikation sind, erfasst werden.⁸ Neben Sprach- und Tastatureingaben können also etwa Bild- oder Videodateien im Zusammenhang mit der gespeicherten Kommunikation durch eine Quellen-TKÜ ermittelt werden.⁹ Zudem wird durch § 100a Absatz 1 Satz 3 StPO festgelegt, dass gespeicherte Inhalte nur erfasst werden dürfen, „wenn sie auch während des laufenden Übertragungsvorgangs im

4 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10.

5 Rückert, in: MüKoStPO, 2. Aufl. 2023, StPO § 100a Rn. 203.

6 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10 f.

7 Freiling/Safferling/Rückert, Quellen-TKÜ und Online-Durchsuchung als neue Maßnahmen für die Strafverfolgung: Rechtliche und technische Herausforderungen, JR 2018, 9, 10.

8 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100a Rn. 123.

9 Henrichs/Weingast, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage 2023, § 100a Rn. 44.

öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können“.

Einen **Sicherungsmechanismus** bei der Vornahme von technischen Eingriffen in informationstechnische Systeme des Betroffenen sieht § 100a Absatz 5 StPO vor:

„Bei Maßnahmen nach Absatz 1 Satz 2 und 3 ist technisch sicherzustellen, dass

1. ausschließlich überwacht und aufgezeichnet werden können:

a) die laufende Telekommunikation (Absatz 1 Satz 2), oder

b) Inhalte und Umstände der Kommunikation, die ab dem Zeitpunkt der Anordnung nach § 100e Absatz 1 auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz hätten überwacht und aufgezeichnet werden können (Absatz 1 Satz 3),

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.“

Aus § 100a Absatz 5 Nr. 1 StPO folgt, dass bereits jede Manipulation des informationstechnischen Systems, die auch nur die technische Möglichkeit beinhaltet, **unabhängig von laufenden Telekommunikationsvorgängen** etwa die Kamera und/oder das Mikrofon von Zielgeräten einzuschalten, von vornherein nicht auf § 100a StPO gestützt werden könnte und insofern **unzulässig** wäre.

Zu beachten sind in diesem Kontext auch die Einschränkungen durch § 100d StPO, der dem **Schutz des Kernbereichs privater Lebensgestaltung** dient. Gemäß § 100d Absatz 1 StPO ist eine TKÜ-Maßnahme unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch eine Maßnahme nach § 100a StPO „allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden“. Werden Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch eine Maßnahme nach § 100a StPO erlangt, dürfen sie nicht verwertet werden; Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen (§ 100d Absatz 2 StPO).

2.2. Online-Durchsuchung

Gemäß § 100b StPO darf auch ohne Wissen des Betroffenen mit **technischen Mitteln** in ein von dem Betroffenen genutztes informationstechnisches System eingegriffen und dürfen Daten daraus erhoben werden (Online-Durchsuchung), wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 StPO bezeichnete besonders schwere Straftat begangen oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat, die Tat auch im Einzelfall besonders schwer wiegt und die Erforschung des Sachverhalts

oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Unter den Begriff des informationstechnischen Systems in diesem Sinne fallen neben klassischen PCs „alle von einem Mikroprozessor gesteuerten Geräte, namentlich auch Mobiltelefone (Smartphones), Organizer oder Server und Router bis hin zu sog. smarten Haushaltsgeräten oder sog. Digitalen Assistenten (zB ‚Alexa‘ von Amazon, ‚Hello‘ von Google, ‚Cortana‘ von Microsoft, ‚Siri‘ von Apple ...).“¹⁰

Zahlreiche Voraussetzungen des § 100b StPO entsprechen denjenigen für die akustische Wohnraumüberwachung nach § 100c StPO.¹¹ So bedarf es einer **Katalogtat** nach § 100b Absatz 2 StPO sowie eines Tatverdachts gegen die Zielperson der Maßnahme. Die Tat muss ebenso im Einzelfall besonders schwer wiegen. Des Weiteren darf keine Subsidiarität gemäß § 100b Absatz 1 Nr. 3 StPO vorliegen, folglich darf keine Ermittlungsmaßnahme mit geringerer Eingriffstiefe aber gleichen Erfolgsaussichten zur Verfügung stehen.¹²

Die Online-Durchsuchung muss sich gemäß § 100b Absatz 3 Satz 1 StPO gegen den **Beschuldigten** richten. Ein informationstechnisches System eines **Dritten** kann **ausnahmsweise** erfasst werden, soweit aufgrund bestimmter Tatsachen anzunehmen ist, dass es vom Beschuldigten benutzt wird und der alleinige Zugriff auf Geräte des Beschuldigten selbst zur Erreichung des Ermittlungsziels nicht genügt (§ 100b Absatz 3 Satz 2 StPO).

Des Weiteren ist die **Verhältnismäßigkeit** einer Anordnung bei deren Erlass sowie beim Andauern der Maßnahme zu überprüfen.¹³ Gemäß § 100e Absatz 5 Satz 1 StPO ist eine Maßnahme abubrechen, sobald der Eingriff nicht mehr im Verhältnis zu den erwarteten Ergebnissen oder zur Schuld des Beschuldigten steht.¹⁴

Liegen die Voraussetzungen des § 100b StPO vor, darf grundsätzlich mit technischen Mitteln in ein von dem Betroffenen der Maßnahme genutztes informationstechnisches System eingegriffen und Daten daraus erhoben werden. Es können nicht nur alle neu hinzukommenden Kommunikationsinhalte, sondern auch alle in dem IT-System gespeicherten Inhalte sowie das Nutzungsverhalten der Person überwacht werden.¹⁵ Insofern ein Betroffener mithin über Smart-Home-Geräte Ton- und/oder Bildaufnahmen erstellt, sind diese von § 100b StPO grundsätzlich erfasst.

Der Begriff der technischen Mittel in § 100b StPO entspricht dabei jenem in § 100a StPO:

10 Henrichs/Weingast, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage 2023, § 100b Rn. 4.

11 Braun/Roggenkamp, 0Zapftis v2.0 Repressive Staatstrojaner, Privacy in Germany (PinG) 7/2019, 53, 56.

12 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 19.

13 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 23.

14 Graf, in: BeckOK StPO, 34. Edition, Stand: 01.07.2019, § 100b Rn. 23.

15 Henrichs/Weingast, in: Karlsruher Kommentar zur Strafprozessordnung, 9. Auflage 2023, § 100b Rn. 5.

„Wie bei § 100a (...) ist der Begriff des technischen Mittels **weit zu verstehen** und umfasst alle Software- und Hardware-Tools, mit denen ein heimlicher Zugriff auf informationstechnische Systeme möglich ist (auch zB Seitenkanalattacken). Hauptanwendungsfall dürfte die Verwendung einer Spähsoftware (sog. Staats- oder Bundestrojaner) sein. Ebenfalls hierunter fällt die Verwendung eines durch die Ermittlungsbehörden anderweitig erlangten Passworts, um heimlichen Zugriff auf ein informationstechnisches System zu erlangen und Daten hieraus zu erheben. Besonders bedeutsam ist dies beim heimlichen Zugriff auf Cloud Server (...) und Heim- oder Firmennetzwerke (...) mittels des jeweiligen Passworts.“¹⁶

Auch bei der Online-Durchsuchung gelten die Grenzziehungen zum **Schutz des Kernbereichs privater Lebensgestaltung** gemäß § 100d Absatz 1 und 2 StPO. Zusätzlich ist gemäß § 100d Absatz 3 Satz 1 StPO, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach § 100b StPO erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind gemäß § 100d Absatz 3 Satz 2 StPO unverzüglich zu löschen oder von der Staatsanwaltschaft dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Im Rahmen einer Online-Durchsuchung erlangte und verwertbare personenbezogene Daten dürfen in **anderen Strafverfahren** ohne Einwilligung der insoweit überwachten Personen nur zur Aufklärung einer Straftat, auf Grund derer Maßnahmen nach § 100b oder § 100c angeordnet werden könnten, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden (§ 100e Absatz 6 StPO).¹⁷

2.3. Zuständigkeit und Verfahren

Gemäß § 100e Absatz 1 StPO darf eine **Quellen-TKÜ** mittels Spähsoftware nur auf **Antrag der Staatsanwaltschaft** durch das **Gericht** angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit eine solche Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ist **auf höchstens drei Monate zu befristen**. Eine Verlängerung um jeweils nicht mehr als drei Monate ist zulässig, soweit die Voraussetzungen der Anordnung unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen.

Bezüglich der **Online-Durchsuchung** legt § 100e Absatz 2 StPO abweichend hiervon fest, dass auch bei Gefahr im Verzug die Staatsanwaltschaft nicht zur Anordnung befugt ist. Vielmehr hat im Regelfall eine bestimmte, nicht mit Hauptverfahren in Strafsachen befasste Kammer des Landgerichts, in dessen Bezirk die Staatsanwaltschaft ihren Sitz hat, und bei Gefahr im Verzug statt der Kammer ihr Vorsitzender die Anordnung zu treffen. Analog zu § 100e Absatz 1 StPO tritt eine solche Anordnung außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird. Die Anordnung ist **auf höchstens einen Monat zu befristen**. Eine Verlängerung um jeweils nicht mehr als einen Monat ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Ermittlungsergebnisse fortbestehen. Ist die Dauer der Anordnung auf

16 Rückert, in: MüKoStPO, 2. Aufl. 2023, StPO § 100b Rn. 35.

17 Zur Verwendung für Zwecke der Gefahrenabwehr trifft § 100e Absatz 6 Nr. 2 und 3 StPO weitere Regelungen.

insgesamt sechs Monate verlängert worden, so entscheidet über weitere Verlängerungen das **Oberlandesgericht**.

In der **Begründung** der Anordnung oder Verlängerung von Maßnahmen nach § 100a StPO und 100b StPO sind deren **Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte** darzulegen (§ 100e Absatz 4 StPO). Liegen die Voraussetzungen der Anordnung nicht mehr vor, so sind die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden und das anordnende Gericht ist nach Beendigung der Maßnahme über deren Ergebnisse zu unterrichten (§ 100e Absatz 5 StPO).

3. Gefahrenabwehr

3.1. Bundespolizei

Die **Bundespolizei** ist **nicht zur Quellen-TKÜ und Online-Durchsuchung** befugt. Einem dahingehenden Gesetzentwurf¹⁸, der vom Bundestag am 10. Juni 2021 angenommen wurde, hat der Bundesrat in der Sitzung vom 25. Juni 2021 die Zustimmung versagt. Im aktuell in der parlamentarischen Beratung befindlichen Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes¹⁹ ist eine Ermächtigung der Bundespolizei für die Quellen-TKÜ oder Online-Durchsuchung nicht vorgesehen.²⁰

3.2. Zollkriminalamt

Durch Gesetzesänderung im Jahr 2021 wurde das **Zollkriminalamt** zur Überwachung und **Aufzeichnung von laufender und ruhender Kommunikation** per **Quellen-TKÜ** berechtigt (§ 72 Absatz 3 Zollfahndungsdienstgesetz – ZFdG²¹).²² Das Zollkriminalamt darf diese Maßnahmen präventiv gegen Personen richten, bei denen der Verdacht eines drohenden Verstoßes gegen die in § 72 Absatz 1 und 2 ZFdG benannten Gesetze über die Kontrolle von Kriegswaffen oder entsprechendes Unionsrecht vorliegt. Abgestellt wird insbesondere auf die Herstellung von und den Handel mit Atomwaffen, biologischen und chemischen Waffen, Antipersonenminen und Streumunition und den ungenehmigten Handel mit Kriegswaffen gem. § 19 Absatz 1 oder 2, § 20 Absatz 1, § 20a Absatz 1 oder 2 oder § 22a Absatz 1 Nummer 4, 5 oder 7 oder Absatz 2 Kriegswaffenkontrollgesetz (KrWaffKontrG)²³. Die Maßnahmen dürfen nur angeordnet werden, wenn es

18 Gesetzentwurf der Fraktionen der CDU/CSU und SPD, Entwurf eines Gesetzes zur Modernisierung der Rechtsgrundlagen der Bundespolizei, [BT-Drs. 19/26541](#) vom 09.02.2021.

19 Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes, [BT-Drs. 20/10406](#) vom 21.02.2024.

20 Barczak, Reform des Bundespolizeigesetzes, ZRP 2023, 148, 148.

21 Gesetz über das Zollkriminalamt und die Zollfahndungsämter vom 30.03.2021 (BGBl. I S. 402), das zuletzt durch Art. 26 des Gesetzes zur Durchführung der VO (EU) 2022/2065 vom 06.05.2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

22 Graulich, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, Abschnitt E Rn. 800.

23 Gesetz über die Kontrolle von Kriegswaffen in der Fassung der Bekanntmachung vom 22.11.1990 (BGBl. I S. 2506), das zuletzt durch Artikel 25 des Gesetzes vom 19.12.2022 (BGBl. I S. 2606) geändert worden ist.

ohne die Erkenntnisse aus den damit verbundenen Maßnahmen aussichtslos oder wesentlich erschwert wäre, die Taten zu verhindern, und die Maßnahmen nicht außer Verhältnis zur Schwere der zu verhindernden Tat stehen (§ 72 Absatz 5 ZFdG).

3.3. Nachrichtendienste

Organisation, Aufgaben und Befugnisse der drei Nachrichtendienste des Bundes, des **Bundesnachrichtendienstes (BND)**, des **Bundesamtes für Verfassungsschutz (BfV)** und des **Militärischen Abschirmdienstes (MAD)** sind jeweils im Gesetz über den Bundesnachrichtendienst²⁴, dem Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz²⁵ sowie dem Gesetz über den Militärischen Abschirmdienst²⁶ geregelt. Nach Maßgabe des Artikel 10-Gesetzes²⁷ sind die Verfassungsschutzbehörden des Bundes und der Länder, der MAD und der BND unter bestimmten Voraussetzungen berechtigt, insbesondere zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes die Telekommunikation zu überwachen und aufzuzeichnen (vgl. § 1 Absatz 1 Artikel 10-Gesetz).

Durch eine Änderung des Artikel 10-Gesetzes im Jahr 2021 wurde die Befugnis zur sogenannte **erweiterte Quellen-TKÜ** für die Nachrichtendienste eingeführt (vgl. § 11 Absatz 1a Artikel 10-Gesetz). Diese dient der Überwachung von Kommunikation über Kommunikationsprogramme, die standardmäßig eine Verschlüsselung ihrer Kommunikationsdaten und -inhalte nutzen. Die Quellen-TKÜ erfasst Kommunikation, bevor diese verschlüsselt oder nachdem diese entschlüsselt wurde bzw. ermöglicht deren Entschlüsselung, indem sie auf das verwendete Endgerät (die „Quelle“) zugreift.²⁸ Dazu bedarf es einer **speziellen Überwachungssoftware**, welche umgangssprachlich als Staatstrojaner bezeichnet wird.²⁹ Dabei erlaubt § 11 Absatz 1a Satz 1 Artikel 10-Gesetz die Überwachung und Aufzeichnung der **laufenden Kommunikation**. § 11 Absatz 1a Satz 2 Artikel 10-Gesetz gestattet darüber hinaus auch die Überwachung der auf dem

24 Gesetz über den Bundesnachrichtendienst (BND-Gesetz – BNDG) vom 20.12.1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 4 des Gesetzes zur Durchführung der VO (EU) 2022/2065 vom 06.05.2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

25 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG) vom 20.12.1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 2 des Gesetzes zur Durchführung der VO (EU) 2022/2065 vom 06.05.2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

26 Gesetz über den militärischen Abschirmdienst (MAD-Gesetz – MADG) vom 20.12.1990 (BGBl. I S. 2954, 2977), das zuletzt durch Artikel 3 des Gesetzes zur Durchführung der VO (EU) 2022/2065 vom 06.05.2024 (BGBl. 2024 I Nr. 149) geändert worden ist.

27 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G 10) vom 26.06.2001 (BGBl. I S. 1254, 2298; 2017 I S. 154), das zuletzt durch Artikel 4 des Gesetzes zum ersten Teil der Reform des Nachrichtendienstrechts vom 22.12.2023 (BGBl. 2023 I Nr. 413) geändert worden ist.

28 Wischmeyer in: Dreier, Grundgesetz-Kommentar, 4. Auflage 2023, Art. 10 Rn. 124.

29 Werner, in: Weber, Rechtswörterbuch, 33. Edition 2024, Stichwort Staatstrojaner; Wissenschaftliche Dienste des Deutschen Bundestages, Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste – Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung, Ausarbeitung vom 19.02.2021, [WD 3 - 3000 - 293/20](#), S. 4.

informationstechnischen System des Betroffenen ab dem Zeitpunkt der Anordnung gespeicherter Inhalte und Umstände der Kommunikation (**ruhende Kommunikation**), wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätte überwacht und aufgezeichnet werden können. Bei diesem Zugriff auf ruhende Kommunikation handelt es sich um die „erweiterte“ **Quellen-TKÜ**, die insofern zum Teil auch als eine beschränkte Online-Durchsuchung bezeichnet und bewertet wird.³⁰ Der Zugriff auf das zu überwachende Gerät kann auch aus der Ferne, das heißt nicht physisch, erfolgen, indem Sicherheitslücken im System des Endgeräts ausgenutzt werden, um die Installation einer Überwachungssoftware zu ermöglichen.³¹

Neben der Quellen-TKÜ gibt es zudem die sogenannte verdeckte **Online-Durchsuchung**, bei der die Behörde ebenfalls mit technischen Mitteln in die von der betroffenen Person genutzten informationstechnischen Systeme (IT-Systeme) eingreift und aus ihnen Daten erhebt. Sie unterscheidet sich von der Quellen-TKÜ darin, dass sie nicht auf die Überwachung laufender oder ruhender Telekommunikation beschränkt ist. Vielmehr können IT-Systeme und Speichermedien ganz unabhängig von Kommunikationsvorgängen online durchsucht und alle verfügbaren Daten gewonnen werden.³² Eine Online-Durchsuchung ist nur bei Bestehen einer besonderen gesetzlichen Ermächtigung zulässig.³³ Seit einer Gesetzesänderung³⁴ des Bundesnachrichtendienstgesetzes im Jahr 2021 ist der BND in den dort genannten Fällen zu Online-Durchsuchungen bei Ausländern im Ausland berechtigt (vgl. § 34 BNDG). Das BfV und der MAD dürfen keine Online-Durchsuchungen durchführen, soweit man nicht die erweiterte Quellen-TKÜ nach § 11 Absatz 1a Satz 2 Artikel 10-Gesetz als Online-Durchsuchung einstuft.

3.4. Bundeskriminalamt

Zur Abwehr von Gefahren des internationalen Terrorismus kann auch das **BKA** auf IT-Systeme zugreifen. Dazu kann es das **Mittel der Quellen-TKÜ einsetzen** (§ 51 Absatz 2

30 Poscher/Kappler, Staatstrojaner für Nachrichtendienste – Zur Einführung der Quellen-Telekommunikationsüberwachung im Artikel 10-Gesetz, Verfassungsblog, 06.07.2021 (<https://verfassungsblog.de/staatstrojaner-nachrichtendienste/>); vgl. auch Wissenschaftliche Dienste des Deutschen Bundestages, Verfassungsrechtliche Fragen zur Regelung des Einsatzes von Quellen-Telekommunikationsüberwachung durch Nachrichtendienste – Entwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts der Bundesregierung, Ausarbeitung vom 19.02.2021, [WD 3 - 3000 - 293/20](#), S. 7.

31 Heckmann/Paschke, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Auflage 2022, § 121 Rn. 86.

32 BVerfGE 120, 274, 38.

33 BVerfGE 120, 274, 328.

34 Gesetz zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 19.04.2021 (BGBl. I S. 771), das zuletzt durch Artikel 58 des Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts sowie des Bundesverwaltungsgerichts vom 23.06.2021 (BGBl. I S. 1858) geändert worden ist.

Bundeskriminalamtgesetz – BKAG³⁵). Zur Durchführung dieser und weiterer Maßnahmen verfügt das BKA sowohl über eigenentwickelte als auch über kommerzielle Software.³⁶ Darüber hinaus kann es **Online-Durchsuchungen** durchführen (vgl. § 49 BKAG). Laut eigener Angaben wird die hierzu verwendete Software einem umfangreichen Testverfahren unterzogen.³⁷

3.5. Berührte Grundrechte und Kontrolle

Sofern der **Zugriff auf ein informationstechnisches System durch den Staat** erfolgt und sich auf die laufende Kommunikation bezieht, ist die Maßnahme an Artikel 10 Grundgesetz (GG)³⁸ zu messen, welcher das **Telekommunikationsgeheimnis** gewährleistet.

Die darüber hinaus gehende Überwachung der Nutzung eines informationstechnischen Systems als solches oder die Durchsuchung von Speichermedien des Systems muss den gesteigerten Anforderungen des **Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (sogenanntes IT-Grundrecht)** gerecht werden, welches das Bundesverfassungsgericht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG abgeleitet hat.³⁹

Im Einzelfall kann auch die **Unverletzlichkeit der Wohnung gemäß Art. 13 GG** betroffen sein, wenn der Computer physisch in der Wohnung manipuliert wird oder wenn IT-Systeme z.B. dafür genutzt werden, Gespräche in Räumen abzuhören.⁴⁰ Darüber hinaus wird in der Literatur vorgebracht, dass es bei der Grundrechtsintensität von Eingriffen auch auf die Art des Trojaners ankomme: Sofern der handelnden Behörde der Quellcode des Trojaners bekannt sei (was regelmäßig nur bei eigener Codierung der Fall sein wird), sei die Eingriffstiefe aufgrund der Bestimmbarkeit der Funktionen besser begrenzt.⁴¹

35 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG) vom 01.06.2017 (BGBl. I S. 1354, ber. 2019 S. 400), das zuletzt durch Artikel 5 des Gesetzes zur Fortentwicklung des Völkerstrafrechts vom 30.07.2024 (BGBl. 2024 I Nr. 255) geändert worden ist.

36 Kipker, Vom Staatstrojaner zum staatseigenen Bundestrojaner, ZRP 2016, 88; Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung: Notwendigkeit, Sachstand und Rahmenbedingungen, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

37 Bundeskriminalamt, Quellen-TKÜ und Online-Durchsuchung: Notwendigkeit, Sachstand und Rahmenbedingungen, abrufbar unter https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html; zu externen Dienstleistern vgl. auch Dickmann/Vettermann, Regelung des behördlichen IT-Schwachstellenmanagements, MMR 2022, 852, 854 f.

38 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes zur Änderung des Grundgesetzes vom 19. Dezember 2022 (BGBl. I S. 2478) geändert worden ist.

39 BVerfGE 120, 274, 302, 314 f.

40 Wischmeyer in: Dreier, Grundgesetz-Kommentar, 4. Auflage 2023, Art. 13 Rn. 96.

41 Kipker, Vom Staatstrojaner zum staatseigenen Bundestrojaner, ZRP 2016, 88, 89.

Die **Zulässigkeitsvoraussetzungen** für die Durchführung einer Quellen-TKÜ oder einer Online-Durchsuchung durch die Nachrichtendienste oder das BKA sind wie oben unter 3.1. bis 3.4. dargestellt in den jeweiligen Gesetzen geregelt. Diese stellen insbesondere **auch technische Anforderungen** an die eingesetzten Mittel.⁴² Die Voraussetzungen gelten jeweils für alle Formen der Quellen-TKÜ und Online-Durchsuchungen, also auch solche, die gegebenenfalls mithilfe von Spionagesoftware durchgeführt werden. Der Einsatz solcher Software muss sich stets an den rechtlichen Maßgaben der Befugnisnormen orientieren.

Zudem enthalten die Gesetze Vorschriften zur **Mitteilung oder Benachrichtigung der betroffenen Personen**. Die Durchführung einer Quellen-TKÜ durch die Nachrichtendienste ist dem Betroffenen nach ihrer Einstellung mitzuteilen. Dies kann jedoch unterbleiben, solange eine Gefährdung des Zwecks der Beschränkung nicht ausgeschlossen werden kann oder solange der Eintritt übergreifender Nachteile für das Wohl des Bundes oder eines Landes absehbar ist (§ 12 Absatz 1 Satz 1 und 2 Artikel 10-Gesetz). Zudem ist der Rechtsweg vor der Mitteilung gemäß § 13 Artikel 10-Gesetz ausgeschlossen. Hinsichtlich Quellen-TKÜ und Online-Durchsuchungen durch das BKA finden sich ähnliche Mitteilungspflichten in § 74 BKAG. Werden hingegen personenbezogene Daten von Ausländern im Ausland durch den BND erhoben, erfolgt grundsätzlich keine Mitteilung an die betroffene Person (§ 59 Absatz 1 BNDG).

Die Tätigkeit des BKA und der deutschen Nachrichtendienste unterliegt **gerichtlicher Kontrolle** sowie der **Fach- und Rechtsaufsicht** der für sie zuständigen Regierungsressorts (Bundeskanzleramt, Bundesministerium des Innern und für Heimat, Bundesministerium der Verteidigung). Für die **parlamentarische Kontrolle**⁴³ der nachrichtendienstlichen Tätigkeit des Bundes gibt es zudem das Parlamentarische Kontrollgremium des Bundestages nach § 14 Artikel 10-Gesetz. Das Parlamentarische Kontrollgremium wiederum wählt die Mitglieder der sogenannten **G 10-Kommission**. Telekommunikationsüberwachungsmaßnahmen der Nachrichtendienste dürfen grundsätzlich nur mit ihrer vorherigen Zustimmung durchgeführt werden (vgl. § 15 Artikel 10-Gesetz). Online-Durchsuchungen des BND bedürfen grundsätzlich der vorherigen Zustimmung durch einen **Unabhängigen Kontrollrat**, der aus ehemaligen Richtern des Bundesgerichtshofs und des Bundesverwaltungsgerichts besteht, die auf Vorschlag der Bundesregierung vom Parlamentarischen Kontrollgremium des Bundestags gewählt werden (§ 37 Absatz 4, § 43 BNDG). Daneben unterliegt die Tätigkeit der Nachrichtendienste auch dem allgemeinen parlamentarischen Fragerecht, der Kontrolle der für das jeweilige Regierungsressort zuständigen Fachausschüsse sowie gegebenenfalls vom Bundestag eingesetzter Untersuchungsausschüsse. Telekommunikationsüberwachungen und Online-Durchsuchungen durch das BKA bedürfen der vorherigen **richterlichen Genehmigung** (§ 49 Absatz 4, § 51 Absatz 3 BKAG).

42 Vgl. etwa § 11 Absatz 1a Satz 3 Nr. 1 Artikel-10 Gesetz; § 49 Absatz 2 BKAG, auf den auch § 51 Absatz 2 BKAG verweist; § 34 Absatz 4 BNDG.

43 Vgl. dazu auch Wissenschaftliche Dienste des Deutschen Bundestages, Parlamentarische Kontrolle der Nachrichtendienste in ausgewählten Staaten, Aktualisierung der Ausarbeitung WD 3 - 3000 - 016/17, [WD 3 - 3000 - 095/22](#), Ausarbeitung vom 14.10.2022.