Sachstand

Rechtsgrundlagen der präventiv-polizeilichen und nachrichtendienstlichen Telekommunikationsüberwachung

[redacted]

Rechtsgrundlagen der präventiv-polizeilichen und nachrichtendienstlichen Telekommunikationsüberwachung

[redacted]

Aktenzeichen: WD 3 - 3000 - 025/16
Abschluss der Arbeit: 27. Januar 2016
Fachbereich: WD 3: Verfassung und Verwaltung

1. Which legal acts regulate the issues concerning the use of the investigative measure interception of communication?

Rechtsgrundlagen für Maßnahmen der präventiv-polizeilichen und nachrichtendienstlichen Telekommunikationsüberwachung finden sich auf Bundesebene insbesondere im Artikel 10-Gesetz[1] sowie in § 23a Zollfahndungsdienstgesetz[2] und § 20l Bundeskriminalamtgesetz[3]. Auf Landesebene enthalten die Landespolizeigesetze einzelner Bundesländer Regelungen über Maßnahmen der Telekommunikationsüberwachung (z.B. Art. 34a ff. Polizeiaufgabengesetz Bayern[4], § 15a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung[5], § 34a Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei[6]).

Die folgende Darstellung beschränkt sich auf Maßnahmen der Telekommunikationsüberwachung im engeren Sinne und klammert die Befugnis zum Abruf von Verbindungsdaten[7] aus, da diese vergleichbaren Regelungen und Vorgaben wie die Telekommunikationsüberwachung im engeren Sinne folgt.

2. Which types of interception of communications are defined (or regulated) by the law (targeted interception, strategic interception)?

Das Artikel 10-Gesetz ermächtigt zum einen zu Maßnahmen der Telekommunikationsüberwachung, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass eine Person bestimmte (insbesondere staatsgefährdende) Straftaten plant, begeht oder begangen hat (§ 3 Artikel 10-Gesetz). Zum anderen regeln §§ 5 ff. Artikel 10-Gesetz die Voraussetzungen für die strategische Überwachung (d.h. eine verdachtslose Fernmeldeüberwachung), die lediglich der Bundesnachrichtendienst durchzuführen berechtigt ist.

---

1 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz), abrufbar unter http://www.gesetze-im-internet.de/g10_2001/index.html (zuletzt abgerufen am 26. Januar 2016).

2 Gesetz über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz), abrufbar unter http://www.gesetze-im-internet.de/zfdg/index.html (zuletzt abgerufen am 26. Januar 2016).

3 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz), abrufbar unter http://www.gesetze-im-internet.de/bkag_1997/index.html (zuletzt abgerufen am 26. Januar 2016).

4 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz), abrufbar unter http://gesetze-bayern.de/Content/Document/BayPAG (zuletzt abgerufen am 26. Januar 2016).

5 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, abrufbar unter http://www.rv.hessenrecht.hessen.de/lexsoft/default/hessenrecht_rv.html?doc.hl=1&doc.id=jlr-SOGHErahmen%3Ajuris-lr00&showdoccase=1&documentnumber=1&numberofresults=138&doc.part=R&doc.price=0.0&paramfromHL=true#docid:169564,1,20151101 (zuletzt abgerufen am 26. Januar 2016).

6 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei (Polizeiaufgabengesetz), abrufbar unter http://landesrecht.thueringen.de/jportal/?quelle=jlink&query=PolAufG+TH&psml=bsthueprod.psml&max=true&aiz=true (zuletzt abgerufen am 26. Januar 2016).

7 Entsprechende Rechtsgrundlagen finden sich insbesondere in § 100g Strafprozessordnung, § 20m Bundeskriminalamtgesetz, § 8a Bundesverfassungsschutzgesetz, § 2a BND-Gesetz, § 4a MAD-Gesetz sowie den Landespolizeigesetzen.

Das Zollfahndungsdienstgesetz, das Bundeskriminalamtgesetz und die Landespolizeigesetze sehen lediglich Maßnahmen der Telekommunikationsüberwachung vor, die sich gegen bestimmte Personen richten.

3. In which cases the measure of interception of communications can be applied (national security related cases, criminal investigation cases)? Is there a different procedure of authorization for different types of cases (national security vs. criminal investigation)? Who authorizes the use of this measure?

Grundsätzlich kann festgehalten werden, dass eine Telekommunikationsüberwachung zu präventiv-polizeilichen Zwecken (z.B. § 20l Bundeskriminalamtgesetz und § 23 Zollfahndungsdienstgesetz), zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes (§ 1 Artikel 10-Gesetz) sowie aus Gründen der Strafverfolgung (§ 100a Strafprozessordnung) zulässig ist. Die verfahrensrechtlichen Voraussetzungen, unter denen eine Telekommunikationsüberwachung zulässig ist, unterscheiden sich je nach Rechtsgrundlage.

Maßnahmen der Telekommunikationsüberwachung zu präventiv-polizeilichen Zwecken bedürfen grundsätzlich der richterlichen Anordnung. Bei Gefahr im Verzug kann die Anordnung durch die Behördenleitung getroffen werden, wobei die richterliche Entscheidung nachzuholen ist. Bei Maßnahmen der Telekommunikationsüberwachung, die auf das Artikel 10-Gesetz gestützt werden, ist folgendes Verfahren vorgeschrieben: Ein Tätigwerden eines der Nachrichtendienste im Anwendungsbereich des Artikel 10-Gesetzes setzt stets einen entsprechenden Antrag der jeweiligen Behörde gemäß § 9 Artikel 10-Gesetz und eine Anordnung nach § 10 Artikel 10-Gesetz voraus. Zuständig für die Anordnung von Beschränkungsmaßnahmen ist bei Anträgen der Verfassungsschutzbehörden der Länder die zuständige oberste Landesbehörde, im Übrigen das Bundesministerium des Innern. Eine besondere Rolle im Verfahren besitzen zwei Gremien des Deutschen Bundestages, das sog. Parlamentarische Kontrollgremium und die sog. G 10-Kommission. Das Parlamentarische Kontrollgremium besteht aus Mitgliedern des Deutschen Bundestages und nimmt für das Parlament die Kontrolle der Nachrichtendienste des Bundes wahr. Die G 10-Kommission besteht nicht zwingend aus Mitgliedern des Deutschen Bundestages und überprüft die von den Nachrichtendiensten durchgeführten Beschränkungen im Bereich des in Art. 10 Grundgesetz garantierten Brief-, Post- und Fernmeldegeheimnisses.

Das Parlamentarische Kontrollgremium wird gemäß § 14 Artikel 10-Gesetz in Abständen von sechs Monaten vom Bundesministerium des Innern über die Durchführung des Artikel 10-Gesetzes unterrichtet. Zudem setzt eine Anordnung strategischer Beschränkungsmaßnahmen nach § 5 und § 8 Artikel 10-Gesetz voraus, dass die jeweiligen Telekommunikationsbeziehungen zuvor vom Bundesministerium des Innern mit Zustimmung des Parlamentarischen Kontrollgremiums bestimmt wurden.

Die G 10-Kommission wird gemäß § 10 Abs. 6 S. 1 Artikel 10-Gesetz monatlich vom Bundesministerium des Innern über die von ihm angeordneten Überwachungsmaßnahmen vor deren Vollzug informiert. Grundsätzlich dürfen daher keine Überwachungsmaßnahmen nach dem Artikel 10-

Gesetz durchgeführt werden, bevor die G 10-Kommission mit der jeweiligen Anordnung befasst worden ist.[8]

4. Which agency/agencies operate the technical systems for interception of communications? Which agencies have access to these systems? Which legal acts regulates these issues?

Derzeit gibt es keine speziellen Behörden, welche die technischen Systeme für die Telekommunikationsüberwachung betreiben. Vielmehr wird die Überwachung der Telekommunikation von der Behörde (ggf. in Zusammenwirken mit dem betroffenen Telekommunikationsanbieter) durchgeführt, die die Telekommunikationsüberwachung beantragt hat. Verschiedene Bundesländer planen jedoch die Einrichtung von länderübergreifenden Telekommunikationsüberwachungszentren, in denen die jeweiligen Landespolizeibehörden bei entsprechenden Maßnahmen zusammenarbeiten sollen.

Die Umsetzung der Überwachungsmaßnahmen durch den jeweiligen Telekommunikationsanbieter ist in § 110 Telekommunikationsgesetz[9] und der Telekommunikations-Überwachungsverordnung[10] geregelt.

5. Which is maximum duration of the period which it is legally allowed to keep the data obtained by interception of communication? How is this data protected and who has access to it?

Im Anwendungsbereich des Artikel 10-Gesetzes verpflichtet § 4 bzw. § 6 Artikel 10-Gesetz die erhebende Stelle, unverzüglich und sodann in Abständen von höchstens sechs Monaten zu prüfen, ob die erhobenen personenbezogenen Daten für die Aufgabenwahrnehmung noch erforderlich sind. Soweit die Daten für diese Zwecke nicht erforderlich sind und nicht für eine Übermittlung an andere Stellen benötigt werden, sind sie unverzüglich unter Aufsicht eines Bediensteten, der die Befähigung zum Richteramt hat, zu löschen. Vergleichbare Regelungen finden sich in den Gesetzen über die verschiedenen Ermittlungsbehörden und Nachrichtendienste.

Fragen des behördeninternen Schutzes und der Zugriffsberechtigung auf die erhobenen Daten sind in der Regel in den nicht allgemein zugänglichen Verwaltungsvorschriften der Stellen geregelt, die die Daten erhoben haben.

---

8 Siehe Huber, in: Schenke/Graulich/Ruthig (Hrsg.), Sicherheitsrecht des Bundes, 2014, § 15 Artikel 10-Gesetz Rn. 52.

9 Telekommunikationsgesetz, abrufbar unter http://www.gesetze-im-internet.de/tkg_2004/index.html (zuletzt abgerufen am 26. Januar 2016).

10 Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation (Telekommunikations-Überwachungsverordnung), abrufbar unter http://www.gesetze-im-internet.de/tk_v_2005/ (zuletzt abgerufen am 26. Januar 2016).

6. Which institution(s) oversights the work of telecommunication service providers, especially on the matters regarding the security of their communication networks from unauthorized interception of communication?

Die Telekommunikationsanbieter sind nach § 109 Telekommunikationsgesetz verpflichtet, die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses sowie zum Schutz personenbezogener Daten zu treffen. Nach § 109 Abs. 2 S. 2 Telekommunikationsgesetz sind insbesondere Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer oder für zusammengeschaltete Netze so gering wie möglich zu halten.

Für die Überprüfung der entsprechenden Sicherheitskonzepte der Telekommunikationsanbieter ist die Bundesnetzagentur zuständig. Als Grundlage für diese Sicherheitskonzepte erstellt die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten.

7. Can you provide us rules of procedures of the special committees/subcommittees responsible for oversight of intelligence agencies? Do those bodies adopt annual plan of activities?

Die parlamentarische Kontrolle der Nachrichtendienste des Bundes wird durch die bereits oben angesprochenen Gremien des Deutschen Bundestages, das Parlamentarische Kontrollgremium und die G-10 Kommission ausgeübt. Lediglich die Geschäftsordnung des Parlamentarischen Kontrollgremiums ist allgemein zugänglich. Sie kann abgerufen werden unter:

http://www.bundestag.de/blob/366638/21f40aeb8bfb9ddf36e01511150a2add/go_pkgr-data.pdf.

Die Kontrolltätigkeit der Gremien gegenüber den Nachrichtendiensten wurde bereits oben unter 3. erläutert. Eine Annahme von jährlich vorgelegten Aktivitätsplänen der Nachrichtendienste durch Beschluss der Gremien erfolgt nicht.

Ende der Bearbeitung