Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

31.01.2012

V-620/057#0146 – VS-NfD

Bericht gemäß § 26 Abs. 2 Bundesdatenschutzgesetz über Maßnahmen der Quellen-Telekommunikationsüberwachung bei den Sicherheitsbehörden des Bundes

Inhalt

A. Zusammenfassung

1. Die Durchführung von Maßnahmen der Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) durch das Bundeskriminalamt (BKA), den Zollfahndungsdienst und die Bundespolizei konnte nur begrenzt datenschutzrechtlich überprüft werden. Zum einen beruht dies auf dem Umstand, dass in der Mehrzahl Quellen-TKÜ im Rahmen strafrechtlicher Ermittlungen auf Weisung einer jeweils zuständigen Staatsanwaltschaft eines Landes vorgenommen wurden, die damit nicht meiner Kontrollkompetenz unterliegen. Zum anderen lagen den genannten Behörden der Quellcode der bei der jeweiligen Maßnahme eingesetzten Software oder eine anderweitige hinreichende Programmdokumentation nicht vor. Belastbare und abschließende Aussagen über die programmierten Funktionen und Zugriffmöglichkeiten der eingesetzten Software sind daher nicht möglich.

2. Aus den vorhandenen Unterlagen ergab sich jedoch, dass die bei Maßnahmen der Quellen-TKÜ eingesetzte Software nicht den Anforderungen der gemäß § 9 Bundesdatenschutzgesetz erforderlichen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes Rechnung getragen haben. Dies gilt insbesondere für die unzureichende Verschlüsselung der anlässlich der Quellen-TKÜ ausgeleiteten Daten und die mangelnde Authentisierung der an den Prozessen beteiligten Personen und Systeme.

3. Bei der Durchsicht der Inhalte der im Zuge der Quellen-TKÜ erlangten Informationen ergaben sich bei keiner der genannten Behörden Anhaltspunkte dafür, dass über die laufende Telekommunikation hinaus Dateninhalte des jeweils infiltrierten Rechners, wie z. B. Bildschirmdarstellungen, durch diese Maßnahmen erlangt worden sind oder dass unzulässige Überwachungsfunktionen aktiviert wurden (z.B. Mikrofone und Kameras zur Raumüberwachung).

4. Unabhängig von der Überprüfung der Einzelmaßnahmen bewerte ich die Frage, ob und inwieweit eine tragfähige Rechtsgrundlage für die Quellen-TKÜ vorliegt, wie folgt: In seinem Urteil[1] zur Online-Durchsuchung fordert das Bundesverfassungsgericht im Hinblick auf die Risiken, die mit einer Quellen-TKÜ verbunden sind, neben technischen Vorkehrungen auch „rechtliche Vorgaben", die den mit der Infiltration des Systems verbundenen Eingriff auf die

[1] BVerfG NJW 2008, 822

Überwachung der Telekommunikation beschränken. Vor diesem Hintergrund stellen § 100a Strafprozessordnung bzw. § 23 a Zollfahndungsdienstgesetz keine hinreichende Rechtsgrundlage für die Durchführung von Maßnahmen der Quellen-TKÜ dar, da diese keine entsprechenden Regelungen enthalten.

5. Die bei Maßnahmen der Quellen-TKÜ durch BKA und Behörden des Zollfahndungsdienstes eingesetzte Software ermöglicht es nicht, die den Kernbereich privater Lebensgestaltung betreffenden Inhalte ausgeleiteter Gespräche gezielt zu löschen. Damit wurde der vom Bundesverfassungsgericht in ständiger Rechtsprechung entwickelte Schutz zum Kernbereichs privater Lebensgestaltung bei heimlicher Telekommunikationsüberwachung, nämlich eine unverzügliche Löschung und Nichtverwertung kernbereichsrelevante Gesprächsinhalte, missachtet.

B. Feststellungen

Im Rahmen meiner Prüfung habe ich zunächst beim Bundeskriminalamt (BKA) am 19./20.10.2011, bei der Bundespolizeidirektion München am 25.10.2011 und beim Zollkriminalamt (ZKA) am 02./03.11.2011 Beratungs- und Kontrollbesuche bzgl. der dort bis dato durchgeführten Maßnahmen der Quellen-Telekommunikationsüberwachung durchgeführt. Den Behörden habe ich die Möglichkeit eingeräumt, vorab zu den von mir festgestellten Sachverhalten Stellungnahmen abzugeben. Diese haben Eingang in den Bericht gefunden.

I. Bundeskriminalamt

Das BKA hat 23 Maßnahmen der sog. Quellen-TKÜ durchgeführt. Davon führte es 19 Maßnahmen in eigener Zuständigkeit sowie vier Maßnahmen in Amtshilfe für andere Behörden durch bzw. bereitete diese vor. Acht der vom BKA in eigener Zuständigkeit durchgeführten Maßnahmen betrafen strafrechtliche Ermittlungsverfahren, elf der Maßnahmen erfolgten zur (vorbeugenden) Gefahrenabwehr. Die in Amtshilfe durchgeführten Maßnahmen betrafen strafrechtliche Ermittlungsverfahren.

Im Rahmen meiner Besuche im BKA wurde mir Einsicht in die Aufnahmeeinheit (Recording Unit) gegeben, wo zu den einzelnen Verfahren die aufgezeichneten personenbezogenen Daten gespeichert waren. Darüber hinaus gewährte mir das BKA Einsicht in die Handakten, soweit diese vorlagen. Schließlich erhielten ich Einblick in alle richterlichen Beschlüsse, die mir zudem in Kopie mit geschwärzten Personennamen übersandt wurden. Zudem haben die Mitarbeiter des BKA während der Kontrollbesuche die Maßnahmen und Hintergründe umfassend erläutert.

1. Allgemeiner Verfahrensablauf

Für die Durchführung der Quellen-TKÜ ist innerhalb des BKA eine Organisationseinheit des kriminalistischen Instituts zuständig (KI 25), die den Bedarfsträger – die jeweilige ermittelnde Einheit des BKA, bzw. in Fällen der Amtshilfe die betreffende Landesbehörde – unterstützt und die Gesamtverantwortung für das Verfahren trägt. Das BKA unterteilt das Verfahren in folgende Phasen:

- **Beratungsphase:** Bevor ein richterlicher Beschluss beantragt wird, berät KI 25 den Bedarfsträger, ob die Durchführung eine Quellen-TKÜ im konkreten Fall sinnvoll erscheint. Dabei werden sowohl kriminaltaktische als auch rechtli-

che Fragen, sowie insbesondere die technische Leistungsfähigkeit und Reichweite der Maßnahme erörtert. Die Anregung gegenüber der ermittlungsführenden Staatsanwaltschaft, einen entsprechenden Gerichtsbeschluss zu beantragen, steht unter dem Vorbehalt der Genehmigung der Amtsleitung. In Fällen der Gefahrenabwehr erfolgt der Antrag auf Erlass einer richterlichen Anordnung durch den Präsidenten des BKA selbst.

- **Vorbereitungsphase:** Das BKA hatte in allen Fällen bereits Vorermittlungen durchgeführt, bevor es richterliche Beschlüsse einholte. Die Vorermittlungen dienten in erster Linie der Feststellung, wie die Zielperson kommunizierte, insbesondere ob sie verschlüsselte Verfahren wie z. B. Skype nutzte. In der Regel werde dazu eine „konventionelle" Telekommunikationsüberwachung des DSL-Anschlusses der Zielperson durchgeführt. Mit deren Hilfe können entsprechende Erkenntnisse aus dem Datenstrom oder aus Kommunikationsinhalten gewonnen werden (siehe im Einzelnen zu IV.). Die Vorermittlungen bezogen sich auch auf das sonstige Nutzungsverhalten und Eigenarten der Zielperson, insbesondere hinsichtlich der Frage, über welche IT-Kenntnisse diese verfügt und in welcher Form diese gegebenenfalls in der Lage ist, Angriffe auf das Zielsystem abzuwehren.

- **Einbringungsphase:** Die Einbringung der Überwachungssoftware (Capture-Unit) erfolge in Abstimmung zwischen KI 25 und dem jeweiligen Bedarfsträger. Bei der Einbringung wird i.d.R. ein Ladeprogramm auf dem Zielsystem zur Ausführung gebracht, durch welches die eigentliche Überwachungssoftware installiert wird. Bevor mit der eigentlichen Maßnahme begonnen wird, muss zunächst das Zielsystem anhand bekannter technischer Parameter verifiziert werden. Jede Einbringung steht unter dem Entscheidungsvorbehalt der Amtsleitung. Die Software werde entweder mittels physischem Zugriff auf das Zielsystem oder auf andere Weise eingebracht. Auf die Darstellung der Einzelheiten wird auf Wunsch des BKA hier verzichtet.

- **Durchführungsphase:** Die Durchführungsphase wird im Einzelnen unter IV. beschrieben. Für die Einhaltung des Schutzes des Kernbereichs privater Lebensgestaltung sind die für die Auswertung der Telekommunikationsüberwachung im BKA allgemein festgelegten Regelungen zu beachten.

- **Beendigungsphase:** Die Capture-Unit wird auf dem Zielsystem gelöscht , wenn die Maßnahme aufgrund taktischer Erwägungen oder wegen Auslaufen des richterlichen Beschlusses beendet werden soll (dazu näher IV.)

- **Nachbereitungsphase:** In der letzten Phase wird die Maßnahme unter technischen und taktischen Gesichtspunkten nachbereitet, um Erkenntnisse für den Einsatz in zukünftigen Fällen zu gewinnen.

2. Verfahren, in den Maßnahmen der Quellen-TKÜ getroffen wurden

a) Strafrechtlichen Ermittlungsverfahren

Die sechs strafrechtlichen Ermittlungsverfahren des BKA, in denen elf Quellen-TKÜ-Maßnahmen vorbereitet bzw. durchgeführt wurden, betrafen unterschiedliche Deliktsbereiche. Gegenstand eines Verfahrens war der Verdacht der Bildung einer kriminellen Vereinigung in Verbindung mit Delikten aus dem Bereich des sog. Phishing (§ 129 StGB nebst weiterer Straftatbestände), in einem weiteren Verfahren der Verdacht der Unterstützung bzw. Mitgliedschaft in einer ausländischen terroristischen Vereinigung (§ 129b StGB). Ein weiteres Verfahren betraf den Verdacht der Vorbereitung einer schweren staatsgefährdenden Gewalttat (§ 89a StGB), zwei Verfahren die Betäubungsmittelkriminalität im Bereich der Organisierten Kriminalität (§ 29a BtMG), ein laufendes Verfahren betraf Betrug im besonders schweren Fall (§ 263 Abs. 1 i.V.m. Abs. 3 StGB).

Das BKA erläuterte, dass §§ 100a, 100b StPO keine näheren Umschreibungen für technische Sicherungen bei der Quellen-TKÜ enthielten. Man orientiere sich aber auch im Bereich der strafprozessualen Maßnahmen an den zusätzlichen Eingrenzungen des § 20l Abs. 2 i.V.m. § 20k Abs. 2 und 3 BKA-Gesetz (BKAG).

b) Verfahren zur Gefahrenabwehr nach §§ 4a, 20l Abs. 2 BKAG

In den vier Maßnahmen, die zum Zwecke der Gefahrenabwehr durchgeführt wurden, lagen dem Bundeskriminalamt Hinweise auf Gefahrenlagen aus dem Phänomenbereich des internationalen Terrorismus vor.

c) Quellen-TKÜ in Amtshilfe für andere Behörden

Das BKA führte vier Maßnahmen zur Quellen-TKÜ in strafrechtlichen Ermittlungsverfahren in Amtshilfe für hessische und rheinland-pfälzische Landespolizeibehörden durch. Diese Verfahren betrafen den Verdacht der Geldwäsche (§ 261 StGB), des Verstoßes gegen das BtMG (§ 29 ff. BtMG), des schweren Bandendiebstahls (§ 244a StGB) und des schweren Raubes (§ 250 StGB).

3. Richterliche Anordnungen

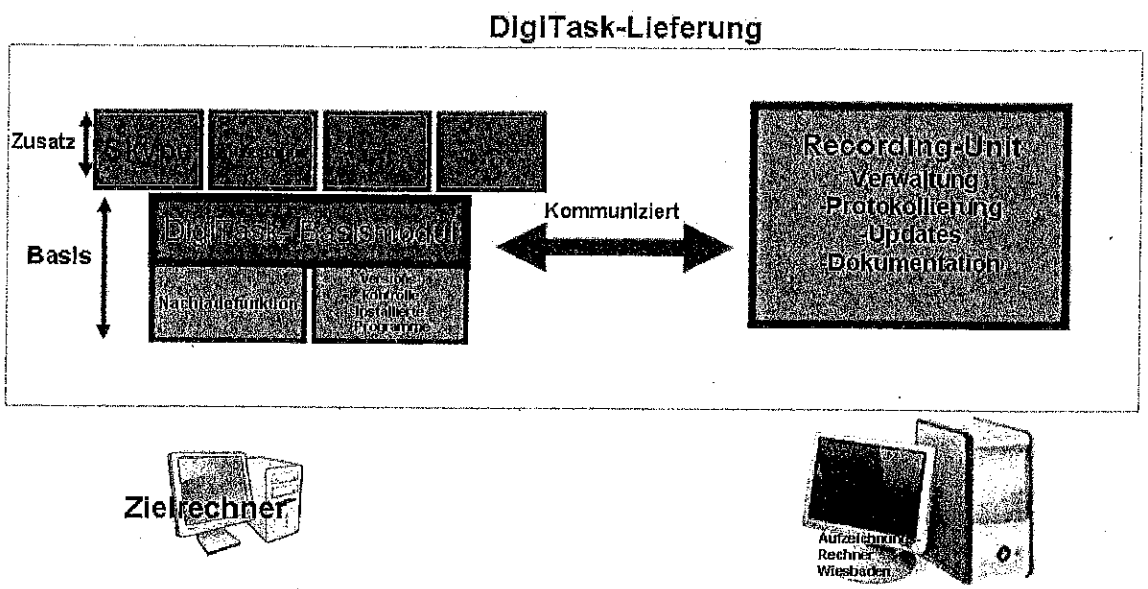
Für alle Maßnahmen sind mir richterliche Beschlüsse vorgelegt worden. Diese sind maßgebend für die datenschutzrechtliche Beurteilung, da die jeweilige Maßnahme nur nach den jeweiligen Vorgaben der gerichtlichen Entscheidung durchgeführt werden darf.

Die Tenorierungen der Beschlüsse sind unterschiedlich. Sie sind teilweise auf sämtliche von der Zielperson genutzten Endgeräte bezogen, teilweise aber auf bestimmte Endgeräte beschränkt. Ein Teil der Beschlüsse begrenzt die jeweiligen Maßnahmen zudem auf bestimmte Telekommunikationsanschlüsse.
In den meisten der Gerichtsbeschlüsse wird zudem in der Tenorierung bzw. in der Begründung darauf hingewiesen, dass eine über die Überwachung und Aufzeichnung der verschlüsselten Telekommunikation hinausgehende „Online-Durchsuchung" des jeweiligen Computers des Betroffenen auszuschließen ist. Zum Teil wird dem Antragsteller ausdrücklich aufgetragen, dass die Funktionsweise des Programms, welches zur Überwachung und Weiterleitung der verschlüsselten Kommunikation verwendet wird, sicherstellen muss, dass die Überwachung und Weiterleitung anderer als der von dieser Anordnung umfassten Daten ausgeschlossen ist, bzw. werden die Ermittlungsbehörden verpflichtet, die genutzte Software entweder selbst fachkundig oder bei Ankauf von einem privaten Hersteller aus eigner technischer Sachkunde auf die Richtigkeit der auf die Quellen-TKÜ beschränkten Funktionsweise hin zu überprüfen. Soweit die Sicherstellung einer solchen Funktionsweise der eingesetzten Software nicht möglich sei, habe die Überwachung insgesamt zu unterbleiben.
Darüber hinaus legen die Beschlüsse zumeist fest, dass Veränderungen am informationstechnischen System nach Beendigung der Maßnahme rückgängig gemacht werden müssen.

4. Beschaffung der Software

Das BKA erstellt die Software für den Quellen-TKÜ-Einsatz nicht selbst, sondern verwendet Software der Firma DigiTask GmbH, mit der ein Rahmenvertrag abgeschlossen wurde. Nach Mitteilung des BKA sei der Markt für die Programmierung von „Überwachungsprogrammen", die für den Einsatz beim BKA geeignet seien, sehr klein. Man habe deshalb auf die Firma DigiTask zurückgegriffen, weil diese am Markt etabliert sei und über einschlägige Erfahrungen verfüge.

Der Rahmenvertrag sieht vor, dass das BKA entsprechende Software mit den gewünschten Funktionen abrufen kann. Jede Version wird individuell angepasst und auch abgerechnet. Die Überlassung des Quellcodes (engl. source code) sieht der Vertrag nicht vor.
Bemerkenswert ist die Formulierung im Rahmenvertrag: „Grundmodul inkl. Skype (Das Modul „Onlinedurchsuchung" ist im Preis enthalten und kann bei Bedarf integriert werden)". Das BKA interpretiert diese Vertragsklausel als deklaratorischen Hinweis, dass die Firma DigiTask ein Modul „Onlinedurchsuchung" in ihrem Portfolio habe, welches technisch integriert werden könne. Tatsächlich habe das BKA dieses Modul niemals abgerufen. Das Modul „Onlinedurchsuchung" sei zu keinem Zeitpunkt Bestandteil der im BKA eingesetzten Software zur Durchführung von Maßnahmen der Quellen-TKÜ gewesen. Für Maßnahmen der Onlinedurchsuchung setze das BKA ohnehin eine andere Software ein.



5. Art der erfassten Inhalte

Zu allen Maßnahmen habe ich das IT-gestützte Auswerteverfahren (zur technischen Beschaffenheit siehe IV.) eingesehen, soweit es nach Angaben des BKA zu einer

Ausleitung von Inhalten gekommen ist. Anhand der Darstellung des Verfahrens war zu jeder Maßnahme ersichtlich, zu welchen Zeitpunkten die Betroffenen online waren und welche Inhalte ausgeleitet wurden. Insbesondere zeigte das System an, welche Inhalte erfasst worden waren: Tonaufzeichnungen, SMS- oder Chat-Inhalte. Bei Durchsicht des IT-gestützten Verfahrens habe ich Audioaufzeichnungen von Gesprächen, die mit entsprechender Software von den Betroffenen über das Internet geführt wurden, insb. mit der Software „Skype"[2], sowie Aufzeichnungen einzelner Chat-Protokolle vorgefunden. Hingegen fanden sich keine Bildschirmdarstellungen (Screenshots) oder Dateiinhalte, die vom infiltrierten Rechner des Beschuldigten erlangt worden waren.

Zu den erfassten Gesprächsinhalten habe ich darüber hinaus die Verschriftung eingesehen. Lediglich in einem Verfahren konnte diese nicht vorgelegt werden. Es handelte sich dabei aber um ein laufendes Verfahren, bei dem die Überwachungsmaßnahme aufgrund der Veröffentlichung des Chaos Computer Clubs (CCC)[3] zum Einsatz von „Trojanern" nach Angaben des BKA gestoppt worden sei.

6. Sensible Inhalte, insb. Kernbereich privater Lebensgestaltung

In einem Verfahren wurde folgender Sachverhalt festgestellt: Es fanden zwei Maßnahmen zur Telekommunikationsüberwachung statt. Zum einen überwachte das BKA den DSL-Anschluss eines Internet-Cafés; diese Überwachung hat nach Mitteilung des BKA neben der umfassenden Einlassung der Beschuldigten maßgeblich zur Aufklärung des Straftatenverdachts geführt.

Zum anderen wurde der mobile Computer des Beschuldigten mittels Quellen-TKÜ überwacht. Diese habe nach Angaben des zuständigen Ermittlungsführers des BKA allerdings keine neuen Erkenntnisse erbracht. Zumeist habe der Beschuldigte über Skype Gespräche mit seiner Freundin in Südamerika geführt. In den Gesprächen sei aber nur sehr abstrakt über Betäubungsmittel gesprochen worden. Die Ergebnisse der Quellen-TKÜ seien von der Staatsanwaltschaft in der Anklage nicht als Beweismittel aufgeführt worden. Vom Gericht wurde die Verurteilung hierauf nicht gestützt.

---

[2] Bei Skype handelt es sich um einen Kommunikationsdienst, bei dem Sprache, Video- und Textinformationen verschlüsselt über das Internet übertragen werden. Voraussetzung ist, dass die Nutzer eine entsprechende Software auf ihren Endgeräten installiert haben und bei dem Diensteanbieter registriert sind.

[3] „Chaos Computer Club analysiert Staatstrojaner", Meldung auf der Website des CCC v. 8.10.2011, http://www.ccc.de/de/updates/2011/staatstrojaner.

Anhand der von uns eingesehenen schriftlichen Aufzeichnungen der Gespräche fanden sich u.a. folgende Zusammenfassungen zu Gesprächen zwischen dem Beschuldigten und seiner Freundin in Südamerika:

- "...kurzes erotisches Gespräch...", 20.11.09, 14:31:54
- „Gespräch übers Wetter und intime Angelegenheiten", 20.11.2009, 15:43:24
- „...Liebesbeteuerungen...", 4.12.2009, 15:46:31, weiterer Wortlaut „...Danach Sexgespräch (Anm. Übers. Ab 15:52:20 bis 16:01:00 finden offensichtlich Selbstbefriedigungshandlungen statt)...", „...weiter privat über Liebe..."

Die Tondateien zu diesen Gesprächen lagen noch vor. Das BKA führte aus, die Staatsanwaltschaft habe verfügt, die Dateien nicht zu löschen. Begründet wurde dies damit, dass eine Teillöschung technisch nicht möglich gewesen sei.

In den übrigen Verfahren hatten zahlreiche der erfassten Gespräche für das Strafverfahren nicht relevante Kommunikation zum Inhalt. Soweit diese Gespräche vom BKA in Schriftform niedergelegt worden waren, beschränkte es sich in der Regel auf kurze, zumeist auf wenige Stichworte begrenzte, Zusammenfassungen (zum Beispiel "privates Gespräch"). Gesprächsgegenstände, die dem Kernbereich privater Lebensgestaltung betreffen könnten, habe ich in den übrigen Verfahren nicht vorgefunden.

Die allgemeine Vorgehensweise zum Schutz des Kernbereichs privater Lebensgestaltung erläuterte das BKA wie folgt: Zunächst markiere der Sachbearbeiter die jeweilige Gesprächsstelle, die er als kernbereichsrelevant ansieht. Diese legt er in dem Kernbereichsbeauftragten (das ist in der Regel der Ermittlungsführer des jeweiligen Verfahrens) vor. Der Kernbereichsbeauftragte bewerte, ob die Stelle tatsächlich als kernbereichsrelevant anzusehen ist, und lege sie gegebenenfalls der Staatsanwaltschaft vor. Diese entscheide darüber, ob der betreffende Gesprächsteil bzw. die Aufzeichnung darüber zu löschen ist.

Das BKA erläuterte, dass die für Maßnahmen der Quellen-TKÜ eingesetzte Software eine gezielte Löschung einzelner Gesprächsteile innerhalb des verwendeten Systems nicht vorsehe. Eine gezielte Löschung würde deshalb voraussetzen, dass die betreffende Tondatei zunächst exportiert werde, um sie anschließend manuell mit einer anderen Software zu bearbeiten. Bei einem solchen Vorgehen würden aber die Dateien aus dem Protokollierungszusammenhang herausgelöst. Inzwischen habe das BKA bei der Fa. DigiTask aber eine Funktion angefordert, mit der einzelne Gesprächsteile innerhalb des Protokollierungszusammenhangs gelöscht werden können. DigiTask habe diese Forderung aber noch nicht umgesetzt.

7. Reichweite

Die auf dem Computer des Beschuldigten installierte Überwachungssoftware leitet die Inhalte zur Überwachungseinheit des BKA unabhängig von den genutzten Telekommunikationsanschlüssen aus. Es ist also unerheblich, ob der Beschuldigte - insbesondere einen mobilen – Computer von zu Hause aus oder in einem Hotel oder an einer anderen Stelle nutzt. Die Telekommunikation wird auch dann überwacht, wenn der Beschuldigte sich im Ausland aufhält.

In der Praxis ist es zur Erfassung von Gesprächen gekommen, die vom Beschuldigten im Ausland geführt wurden. Konkret hat der Beschuldigte zumindest in den oben erwähnten Verfahren mit seinem Laptop auch vom Ausland aus mit seiner Freundin telefoniert. In Bezug auf die Datenerhebung im Ausland wurde erläutert, dass seitens des BKA nicht immer eindeutig bestimmt werden könne, ob Daten im In- oder Ausland erhoben werden. Allein auf Grund der verwendeten IP-Adresse[4] sei eine solche Zuordnung nicht sicher möglich, denn insoweit seien die Geo-IP-Datenbanken nicht immer genau. Deren Datenbasis sei auf Grundlage von massenhaft, aber dennoch individuell erhobenen Erfahrungswerten zusammengetragen und solle einen möglichst präzisen – aber dennoch nicht verbindlichen Zusammenhang zwischen IP-Adressen und geografischen Informationen herstellen. Eine näherungsweise Ableitung einer derartigen Information sei allenfalls im Rahmen der Zuordnung einer IP-Adresse zu einem Adresskontingent eines bestimmten Providers (per sog. „Whois-Abfrage") bzw. bei der Verfolgung des Wegs von IP-Datenpaketen im Internet zu einer bestimmten IP-Adresse (per. sog. „Traceroute") möglich.

Das BKA teilte mit, dass hinsichtlich der Unsicherheiten bei möglichen Auslandsaufenthalten im konkreten Verfahren der Staatsanwaltschaft die eingeschränkten technischen Gegebenheiten dargestellt worden seien. Diese habe daraufhin entschieden, dass die Maßnahme aufgrund der technischen Unsicherheiten im vollen Umfang weiterzuführen sei. Im genannten Fall seien aber Erkenntnisse aus Begleitmaßnahmen vorhanden gewesen seien, wonach der Beschuldigte auch aus dem Ausland über Skype kommunizierte. Daher sei mit der Staatsanwaltschaft abgesprochen worden, dass gegebenenfalls im Nachhinein im Wege der internationalen Rechtshilfe Genehmigungen eingeholt werden sollten, soweit die Ergebnisse beweiserheblich würden. Dazu sei es aber nicht gekommen, da die Skype-Gespräche letztlich für die strafrechtliche Entscheidung nicht tragend waren.

[4] IP (Internet Protocol)-Adressen identifizieren die Rechner, die die Kommunikation abwickeln oder an ihr beteiligt sind. Sie ermöglichen das Senden und Empfangen von Datenpaketen über das Internet.

Das BKA vertritt die Auffassung, in Fällen, in denen unzweifelhaft feststeht, dass sich das überwachte Endgerät im Ausland befindet, sei grundsätzlich ein justizielles Rechtshilfeersuchen an den betroffenen Staat zu stellen.

8. Zeiträume

In einem Verfahren gab das BKA an, dass aufgrund der Anordnung des Generalbundesanwalts (GBA) die Maßnahme am 16.12.2010 enden sollte, tatsächlich die Überwachungssoftware aber erst am 26.1.2011 im Remote-Zugriff entfernt werden konnte. Aus den Protokolldaten sind aber Online-Zeiten ersichtlich, die deutlich über den 16.12.2010 hinausgehen. Ab dem 16.12.2010 ist aber keine Gesprächsaufzeichnung ersichtlich. Zu diesem Zeitpunkt habe die Bundesanwaltschaft die Beendigung der Maßnahme angeordnet. Es sei aber aus technischen Gründen in diesem Fall nicht möglich gewesen, die Überwachungssoftware auf dem Zielsystem per Fernzugriff zu löschen. Daher sei die in der eingesetzten Überwachungssoftware implementierte Funktion zur Aufzeichnung von Telekommunikationsinhalten zu diesem Datum deaktiviert worden. Die anderen Funktionen der Überwachungssoftware, die Rückmeldung ihrer Präsenz und Funktionsbereitschaft, auf dem in Betrieb befindlichen Zielsystem an die Recording Unit zu übermitteln, blieb insoweit aber bis zur manuellen Löschung auf dem Zielsystem am 26.01.2011 erhalten.

II. Zollkriminalamt/Zollfahndungsdienst

Das ZKA und die Zollfahndungsämter (ZFÄ) haben insgesamt 16 Maßnahmen zur Quellen-TKÜ durchgeführt. Vier Maßnahmen erfolgten durch das ZKA in eigener Zuständigkeit, die übrigen zwölf durch die ZFÄ. Drei der vom ZKA durchgeführten Maßnahmen waren auf die Gefahrenabwehr gemäß § 23a Zollfahndungsdienstgesetz (ZFdG) gerichtet, eine erfolgte im Rahmen eines Ermittlungsverfahrens auf der Grundlage von § 100a StPO. Sämtliche Quellen-TKÜ-Maßnahmen der ZFÄ wurden im Rahmen von strafrechtlichen Ermittlungsverfahren durchgeführt. Alle genannten 16 Maßnahmen betrafen die Überwachung von „Skype-Kommunikation".

Bei meinem Besuch wurde mir Einsicht in die Aufnahmeeinheit (Recording Unit) gegeben, wo zu einzelnen Maßnahmen die aufgezeichneten Gespräche gespeichert waren. Darüber hinaus gewährte mir das ZKA Einsicht in die Handakten, soweit diese vorlagen. Schließlich erhielt ich Einblick in richterliche Beschlüsse, die mir zudem in Kopie mit geschwärzten Personennamen übergeben wurden. Ich erhielt auch Kopien der Verträge und Vergabeunterlagen mit den Firmen DigiTask und ERA Soluti-

ons, die Hard- und Software-Komponenten für die technische Umsetzung der Quellen-TKÜ-Maßnahmen lieferten. Zudem haben die Mitarbeiter des ZKA die Maßnahmen und deren Hintergründe umfassend erläutert.

1. Allgemeiner Verfahrensablauf/Organisation

Zwischen dem ZKA und den ZFÄ gibt es gem. § 1 Abs. 1 ZFdG eine organisatorische Trennung mit der Folge, dass Maßnahmen der Quellen-TKÜ vom ZKA und den ZFÄ jeweils eigenständig durchgeführt werden. Innerhalb des ZKA ist für rechtliche Angelegenheiten das Referat II 1 und für die technischen Belange das Referat II 5 zuständig. Diese unterstützen auch die ZFÄ bei der Durchführung von Quellen-TKÜ-Maßnahmen.

Eine Ausnahme von der o.g. organisatorischen Trennung zwischen dem ZKA und den ZFÄ ist die Beschaffung der notwendigen Hard- und Software. Diese wird zum Teil vom ZKA für die ZFÄ mitbeschafft (Näheres siehe 4 a.).

2. Verfahren, in denen Maßnahmen der Quellen-TKÜ getroffen wurden

a) Strafrechtliche Ermittlungsverfahren

Ein Ermittlungsverfahren des ZKA erfolgte gem. § 100a StPO wegen einer Straftat gegen das Außenwirtschaftsrecht (§ 34 Außenwirtschaftsgesetz -AWG). Hierbei sei das genutzte Spähprogramm jedoch nicht aktiviert worden.

Die Ermittlungsverfahren der ZFÄ richteten sich gegen nachfolgende Straftaten: Gewerbs- und bandenmäßiger Schmuggel von Arzneimitteln
(§ 373 AO, § 95 Abs. 1 Nr. 1 ArzneimittelG), Handel und Einfuhr mit Betäubungsmitteln (§§ 29 ff. BtMG), gewerbsmäßige und bandenmäßige Steuerhinterziehung durch Schmuggel von Zigaretten (§§ 369, 370, 373, 374 AO), Bildung einer kriminelle Vereinigung, gewerbsmäßige und bandenmäßige Steuerhinterziehung durch Schmuggel von Zigaretten (§ 129 StGB, §§ 369, 370, 373, 374 AO).

Bei neun von zwölf Maßnahmen der ZFÄ wurden „Trojaner" erfolgreich aktiviert. Bei sieben Maßnahmen übermittelten Trojaner Daten an die ZFÄ. Ein Grund dafür, dass in den anderen Verfahren keine Daten angeliefert worden seien, könnte nach den Erläuterungen des ZKA darin liegen, dass seitens des Betroffenen ein neues System

auf dem infiltrierten Computer aufgespielt worden sei, wodurch der „Trojaner" gelöscht worden sein könnte.

Soweit die Betroffenen der Maßnahmen zu benachrichtigen waren, ist dies nach Auskunft des ZKA jeweils durch die ermittlungsleitende Staatsanwaltschaft erfolgt.

b) Verfahren zur Gefahrenabwehr nach §§ 23a ff. ZFdG

In den drei Maßnahmen, die zum Zwecke der Gefahrenabwehr durchgeführt wurden, lagen dem Zollkriminalamt nach eigenen Angaben Hinweise auf Gefahrenlagen vor. Sie betrafen Verstöße gegen § 34 AWG. Es lagen insoweit richterliche Beschlüsse zur Durchführung von Maßnahmen nach §§ 23a ff. ZFdG vor.

Nach Auskunft des ZKA sei bei keinem der drei ZKA-Maßnahmen das genutzte Spähprogramm (Trojaner) erfolgreich aktiviert worden. Somit seien auch keine Daten von Computern Betroffener an das ZKA übermittelt worden.

3. Richterliche Anordnungen

Für den Inhalt der richterlichen Anordnungen gilt das unter I. 3. Ausgeführte entsprechend.

4. Beschaffung der Hard- und Software

Die Beschaffung von Hard- und Software für Maßnahmen der Quellen-TKÜ erfolgte von privaten Anbietern. Dies geschah bis 2007 bei der Firma ERA Solutions, danach bei der Firma DigiTask. Für jede „Quellen-TKÜ" wurde eine gesonderte Beschaffungsmaßnahme durchgeführt, ein Rahmenvertrag existiert nicht. Die technischen Anforderungen wurden durch das ZKA bzw. durch das jeweilige ZFA eigenständig festgelegt

Zum Inhalt der zur Verfügung gestellten Vergabeunterlagen zu den einzelnen Quellen-TKÜ-Maßnahmen ist Folgendes zu bemerken:

Inwieweit die hierfür durchgeführte Beschaffung die Grenzen des Gerichtsbeschlusses einhält, lässt sich aus den vorgelegten Vertragsunterlagen mit den Firmen ERA und DigiTask nicht feststellen. Insbesondere die Prüfung der Funktionsweise der

eingesetzten „Spähsoftware" lässt sich daraus nicht erschließen. Die Vertreter des ZKA erklärten hierzu, dass durch Tests die Skype-bezogenen Funktionalitäten sowie der Infektionsfähigkeit und der Entfernbarkeit des Trojaners durch die berechtigte Stelle überprüft worden sei. Eine weitergehende Überprüfung im Hinblick auf Funktionsweisen, die die Software über die Überwachung der laufenden Telekommunikation hinaus haben könnte, sei dem ZKA technisch nicht möglich gewesen, da der Quellcode der Überwachungssoftware der Unternehmen ERA und DigiTask nicht vorgelegen habe.

Das Unternehmen DigiTask habe mit Schreiben vom 11.10.2011 sowie in vorangegangenen Gesprächen und Besprechungen versichert, dass der Zollfahndungsdienst eine Software nutzt, die ausschließlich die Überwachung von Telekommunikation (hier: Skype Telekommunikation) ermöglicht. Weitere Funktionalitäten, wie z.B. Screenshots fertigen, wären nicht implementiert.

Das genannte Schreiben der Fa. DigiTask wurde mir anlässlich meines Besuchs im ZKA nicht vorgelegt. Lediglich im Zusammenhang mit einer Maßnahme des ZFA Hannover ist aus einem Vermerk des ZFA zu Auftragsvergabe zu entnehmen, dass von den Firmen ERA Solution und DigiTask bestätigt worden sei, dass „eine Online-Durchsuchung nicht möglich sei".

5. Art der mit der Maßnahme erfassten Inhalte

Bezüglich der Art der mit der Maßnahme erfassten Inhalte wird auf das unter I. 5. Ausgeführte verwiesen.

Bei der Durchsicht der Inhalte fanden sich insbesondere keine von den Anordnungen nicht gedeckte Bildschirmdarstellungen (Screenshots) oder Dateiinhalte, die vom infiltrierten Rechner des Beschuldigten erlangt worden waren.

6. Sensible Inhalte, insb. Kernbereich privater Lebensgestaltung

Zu den erfassten Gesprächsinhalten habe ich stichprobenartig auch die Verschriftung eingesehen. Dabei haben sich keine Anhaltspunkte ergeben, dass es bei der Überwachung und Aufzeichnung der Telekommunikation zu Verletzungen des Kernbereichs privater Lebensgestaltung der Betroffenen gekommen ist.

Die allgemeine Vorgehensweise zum Schutz des Kernbereichs privater Lebensgestaltung erläuterte das ZKA wie folgt: Der Sachbearbeiter markiere die jeweilige Ge-

sprächsstelle, die er als kernbereichsrelevant ansieht. Diese lege er dem Staatsanwalt (in repressiven Maßnahmen) oder dem Maßnahmeleiter (in präventiven Maßnahmen; dies ist eine Person mit Befähigung zum Richteramt) vor. Der Ermittlungsleiter bewerte, ob die Stelle tatsächlich als kernbereichsrelevant anzusehen ist, und entscheide darüber, ob der betreffende Gesprächsteil bzw. die Aufzeichnung darüber zu löschen ist.

Das ZKA erläuterte, dass auch die zum Zeitpunkt meines Besuchs für Maßnahmen der Quellen -TKÜ im Zollfahndungsdienst eingesetzte Software es technisch nicht ermögliche, einzelne Gesprächsteile aus den Datenbanken zu löschen, ohne dass dadurch der Protokollierungszusammenhang beschädigt würde (vgl. I.6). Bei Gesprächen mit der Firma DigiTask sei eine Funktion angefordert worden, mit der man auch einzelne Gesprächsteile innerhalb des Protokollierungszusammenhangs löschen könne. DigiTask habe dies aber noch nicht umgesetzt. Eine gezielte Löschung bestimmter Gesprächsteile bei IP-basierter Telekommunikation sei erst mit einer späteren der Software-Version vorgesehen.

7. Reichweite

Auf die Ausführungen unter I. 7. wird verwiesen.
Nach dem Aufspielen der Überwachungssoftware auf dem Computer des Beschuldigten konnten ausschließlich Telefonate zwischen dem Täter und seiner im europäischen Ausland aufhältigen Verlobten überwacht werden. Der überwachte Computer sei ausschließlich von der Verlobten genutzt worden. Nach Rücksprache mit der Staatsanwaltschaft sei die Software umgehend per Löschbefehl deinstalliert worden, da für die Überwachung ein Rechtshilfeersuchen notwendig gewesen wäre. Die aufgezeichneten Gespräche seien gelöscht worden.

Die Gerichtsbeschlüsse des zuständigen Amtsgerichts bezogen sich auf Festnetzanschlüsse und Mobilfunknummern des Beschuldigten. Bei dieser Maßnahme wurde die Software auf dem Computer des Beschuldigten aber erst installiert, als dieser sich im europäischen Ausland aufhielt und somit einen anderen Telefonanschluss benutzte. Ausweislich eines Aktenvermerks wurden deshalb die Beschlüsse des Amtsgerichts im Wege der Rechtshilfe den dortigen Behörden übermittelt und dort in nationale Gerichtsbeschlüsse umgesetzt.

8. Löschung

Die Überwachungssoftware auf dem Zielrechner muss bei Beendigung der Maßnahme gelöscht werden. Dies erfolge entweder per Fernsteuerung („Remote-Modus") oder durch physischen Zugriff. Die Löschung durch physischen Zugriff erfolge bei Ermittlungs- und Kontrollmaßnahmen der Zollverwaltung.

III. Bundespolizei

Die Bundespolizei hat bislang nur in einem Fall eine Quellen-TKÜ durchgeführt. Einen entsprechenden Beschluss zu deren Durchführung hat die Bundespolizeidirektion München über die zuständige Staatsanwaltschaft auf der Grundlage des § 100a StPO im Rahmen eines Ermittlungsverfahrens aus dem Bereich der Schleusungskriminalität am 3. April 2008 erwirkt. Konkret wurde dem betreffenden Beschuldigten (gemeinsam mit anderen Beschuldigten) das gewerbs- und bandenmäßige Einschleusen von Ausländern gem. § 97 Abs. 2 Aufenthaltsgesetz vorgeworfen. In dem vom Amtsgericht München am 3. April 2008 gegen den Beschuldigten erlassenen Beschluss wird die Überwachung und Aufzeichnung der über den genannten Anschluss geführten Telekommunikation sowie die Vornahme der hierzu erforderlichen Maßnahmen im Rahmen einer Fernsteuerung" anordnet. Dabei wird betont, das nur die laufende Telekommunikation abgehört werden darf, das Durchsuchen des betreffenden Computers dagegen unzulässig ist.

Zur technischen Durchführung der Quellen-TKÜ hat die Bundespolizei das Bayerische Landeskriminalamt (BLKA) um Unterstützung ersucht. Dabei habe die Bundespolizei nach eigenen Angaben mündlich darauf hingewiesen, dass nur laufende Telekommunikation erfasst werden dürfe. Schriftliche Abmachungen wurden nicht getroffen. Genauere Erkenntnisse dazu, mit Hilfe welcher Software das BLKA die Maßnahme technisch umgesetzt hat, liegen der Bundespolizei nicht vor.

Im Ergebnis wurden zwischen dem 14. Mai 2008 und dem 2. Juli 2008 an 43 Tagen Daten aus der Maßnahme ausgeleitet. Die Beendigung der Maßnahme erfolgte durch Fernsteuerung.
Während der laufenden Maßnahme brannte das BLKA die aus der Überwachungsmaßnahme erlangten Dateien auf CDs und übergab diese der Bundespolizei. Insgesamt wurden 13 Datenträger übermittelt, die mit einer speziell dafür bereitgestellten Software ausgewertet wurden.

Die im Rahmen des o.g. Beratungs- und Kontrollbesuchs gesichteten Datenträger und die dazu erstellten Verschriftlichungen enthielten nur Gesprächsinhalte aus der vom Beschuldigten geführten Internettelefonie. Anhaltspunkte dafür, dass mittels der vom BLKA aufgespielten Software auch auf sonstige auf dem betreffenden Computer gespeicherte Daten zugegriffen und ausgeleitet wurden, ergaben sich nicht.
Die Bundespolizei hat während der Durchführung der Maßnahme nach eigenen Angaben keine kernbereichsrelevante Kommunikation aufgezeichnet. Aus den Stichproben, die im Rahmen der Kontrolle nachgelesen bzw. nachgehört wurden, ergeben sich keine anderen Erkenntnisse.

Das Strafverfahren gegen den Beschuldigten wurde in der Zwischenzeit abgeschlossen. Nach Aussage der Bundespolizei sei er zu einer dreijährigen Haftstrafe verurteilt worden. Die aus der Quellen-TKÜ gewonnenen Erkenntnisse seien dabei nicht verwertet worden. Die Benachrichtigung sei durch die Staatsanwaltschaft erfolgt, ohne dass weitere Kenntnisse dazu vorliegen. Eine Anordnung der Staatsanwaltschaft zur Löschung der durch die verschiedenen Telekommunikationsüberwachungen aufgezeichneten Gespräche sei noch nicht erfolgt.

IV. Technische Durchführung

1. BKA

a) Dokumentation der Software beim BKA

Das BKA hat – mangels Kenntnis des Quellcodes – keinen lesbaren, in einer Programmiersprache geschriebenen Text der eingesetzten Software, sondern nur die von einem Computer in Maschinensprache übersetzte Variante (Binärcode).
Eine Einsichtnahme in den Quellcode durch das BSI bzw. eine Prüfung des Quellcodes durch das BSI hat in keinem Fall stattgefunden.

Die von DigiTask bezogene Software besteht im Wesentlichen aus einem Basis-Modul, das die Nachladefunktion umfasst und einer Funktion zum Ermitteln der installierten Software auf dem Zielrechner, sowie Zusatzmodule für die jeweilige eingesetzte Kommunikationssoftware. Ob die Software darüber hinaus noch über weitere Funktionalitäten verfügt, konnte aufgrund des fehlenden Quellcodes nicht festgestellt werden – weder durch das BKA noch durch mich.

Meine Mitarbeiter haben bereits während des Kontrollbesuches um den Quellcode der Software zum Zwecke der datenschutzrechtlichen Kontrolle gebeten. Dieser Bitte konnte das BKA zunächst nicht Rechnung tragen, da es über keine Kopie des Quellcodes verfügte.
Nachdem in der Presse bekannt wurde, dass die Firma DigiTask dem Bayerischen Landesbeauftragten für den Datenschutz Einsicht in den Quellcode gestatten wolle, habe ich das BKA mit ergänzendem Schreiben vom 12.12.2011 unter Hinweis darauf nochmals gebeten, mir den Quellcode zur Verfügung zu stellen. Mit Schreiben vom 17.01.2012 teilte mir das BKA mit, dass die Firma DigiTask grundsätzlich bereit sei, Einblick in den Quellcode zu gewähren. Dies könne jedoch nur, so die Vorgabe von DigiTask, in den Räumlichkeiten der Firma erfolgen. DigiTask und BKA würden jedoch Personal bereitstellen, um Fragen zu beantworten. Ich beabsichtige, auf dieses Angebot einzugehen. Um den Bericht gegenüber dem Deutschen Bundestag nicht ungebührlich zu verzögern, habe ich jedoch zunächst davon abgesehen, die Ergebnisse der ergänzenden Prüfung abzuwarten. Über die Ergebnisse der Kontrolle des Quellcodes werde ich nachberichten.

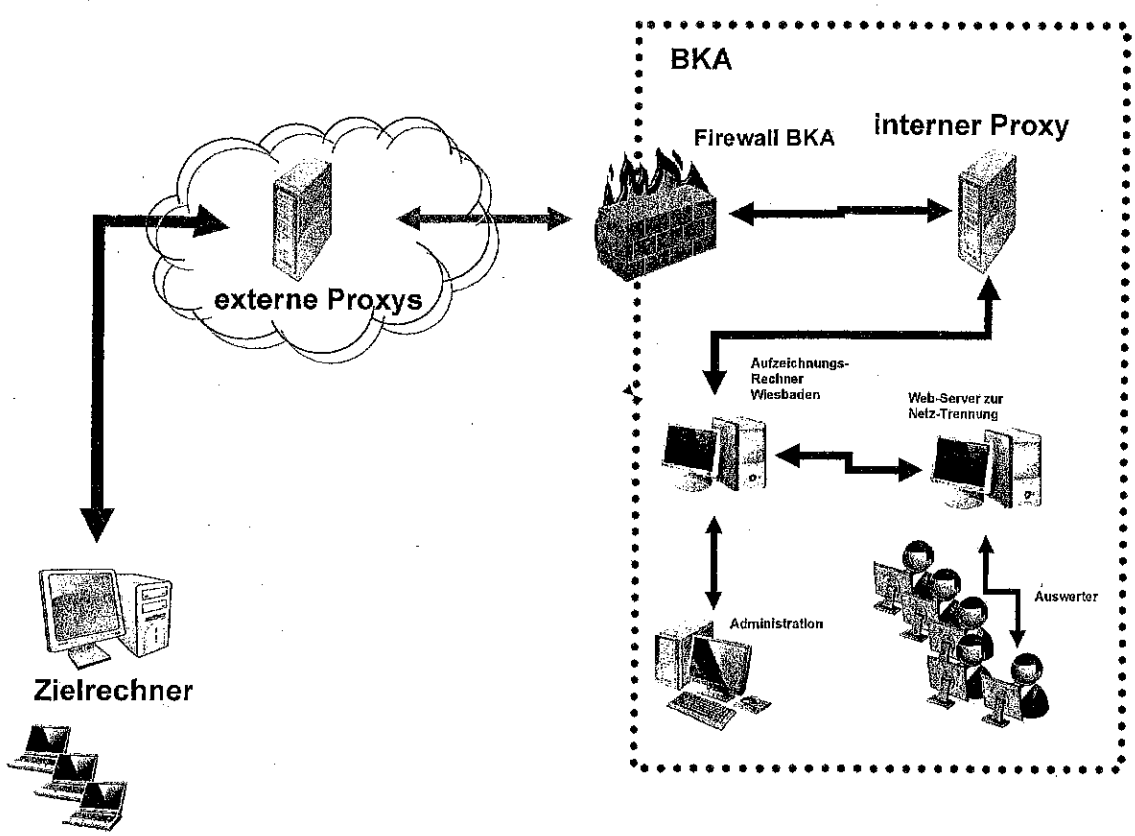
b) Einsatzablauf

Sind die Einsatzbedingungen für die Quellen-TKÜ-Software bekannt (Hardware, Betriebssystem/-Release, Kommunikationssoftware, Virenscanner etc.) wird DigiTask beauftragt, eine entsprechende ausführbare Datei (Binärdatei) mit den bestellten Funktionalitäten bereitzustellen. Anschließend wird eine Software ohne Aufzeichnungsfunktion geliefert. Diese hat nur die Nachladefunktion und eine Funktion zur Auflistung der Software des infizierten Rechners. Mit einem ebenfalls von DigiTask bezogenen Programm werden die IP-Adresse eines externen Proxy-Systems und ggf. die sogenannte U-Nummer – das interne Kennzeichnen der Maßnahme im BKA – als Identifizierungsmerkmal in die Binärdatei eingefügt. Die Software wird zunächst vom BKA soweit wie möglich unter ähnlichen Bedingungen (Hardware, Software) getestet. Sofern die Tests die Funktionalität der Software ergeben, wird diese vom BKA freigegeben. Die Freigabe wird elektronisch in einem Web-Tagebuch vermerkt.

Anschließend wird diese erste Komponente der Überwachungssoftware auf den bzw. die Zielrechner aufgebracht (siehe oben unter 1. Einbringungsphase).

Nach der Rückmeldung des Zielrechners mit seiner MAC-Adresse oder – wenn vorhanden – der oben genannten U-Nummer am Aufzeichnungsrechner prüft das BKA per Fernzugriff die Softwarekonfiguration des Zielrechners, um zu verifizieren ob das richtige System „infiziert" wurde und um die Kompatibilität der zur Verwendung vor-

gesehenen Überwachungssoftware nochmals abzuschätzen. Anschließend wird Software mit den eigentlichen Überwachungsfunktionen und die U-Nummer – falls diese noch nicht zugewiesen wurde – in Form eines Updates nachgeladen. Die Kommunikation läuft über externe Proxy-Server, eine BKA-eigene Firewall und einen internen Proxy-Server auf den Aufzeichnungsrechner.[5] Die Kommunikation ist laut BKA mit dem Verschlüsselungsverfahren AES gesichert. Die Güte der Verschlüsselung wurde allerdings nur grob geprüft (siehe unten d)). Die IP-Adresse bestimmter externen Proxy-Server ist konfigurierbar. Dieser Server muss auch von außen, d.h. vom Internet erreichbar sein. Alle externen Proxy-Server standen – laut Auskunft des BKA – unter seiner exklusiven Kontrolle. Sollten sich bei der ersten Kommunikation Schwierigkeiten zeigen, wird in der Regel ein Nachladeprozess angestoßen. Die Software wird durch Updates an die Erfordernisse des BKA angepasst. Von Seiten des BKA wurde explizit darauf hingewiesen, dass nur Funktionalitäten die die Software besser an die Zielumgebung anpassen, evtl. auch eine Version zur Überwachung einer weiteren Internettelefonieanwendung, jedoch keine Erweiterung der Funktionalitäten im Sinne einer Onlinedurchsuchung nachgeladen werden.



[5] Ein Proxy-Server ist ein Kommunikationsrechner, der als Vermittler arbeitet. Auf der einen Seite nimmt der Proxy Anfragen entgegen, um dann über seine eigene Adresse eine Verbindung zu einer anderen Seite herzustellen.

c) Proxy-Server

Die auf den Zielsystemen aufgebrachte Nachlade- und Überwachungssoftware wird über das Internet von einem im BKA betriebenen Server (Recording Unit) gesteuert. Nach Mitteilung des BKA wurden – als Zwischenstationen - auch im Ausland betriebene Proxy-Server genutzt. Auch diese liefen unter der Verantwortung des BKA. Für unterschiedliche Maßnahmen seien jeweils eigene Server angemietet worden. Der genaue Standort der verwendeten Server war bei der Prüfung nicht mehr verifizierbar.

d) Verschlüsselung der Datenströme (Up-Download)

Laut Auskunft BKA verwendet DigiTask das AES Block-Cipher-Verfahren zur Verschlüsselung von Daten, die über das Internet übertragen werden. Das BKA habe die Verschlüsselung nur „grob" dahingehend überprüft, ob der Datenstrom überhaupt verschlüsselt wird. Dazu fand eine Klartextprüfung statt: Danach wird sowohl der Ausgangs- wie Eingangsdatenstrom mit AES verschlüsselt. AES ist ein symmetrisches Verfahren, d.h. zum Ver- und Entschlüsseln wird der gleiche Schlüssel verwendet. Wie der CCC festgestellt hat, befindet sich dieser Schlüssel bei der ihm zugespielten Software im Programmcode (in einer DLL-Datei). Ich habe im BKA mit Hilfe eines speziellen Editors (HEX-Editor) denselben AES-Schlüssel gefunden. Der AES-Schlüssel der Software beim BKA entspricht der vom CCC untersuchten Variante.

Insofern sehe ich starke Anhaltspunkte dafür, dass die Steuerung des Zielrechners, insb. der Up- und Download nicht nur mit einem für Dritte leicht zu findenden Schlüssel verschlüsselt, sondern dass auch mit einer unzureichenden Implementierung des AES-Verfahren gearbeitet worden sein könnte. Eine Prüfung war für mich ohne die Analyse des Quellcodes bislang nicht möglich. Eine Prüfung oder eine Beratung durch das BSI hat nicht stattgefunden. Auch im Nachgang zu meiner Kontrolle hat das BKA nicht mitgeteilt, welcher Schlüssel bei den Überwachungsmaßnahmen tatsächlich verwendet wurde und ob insoweit meine Annahme zutrifft.

e) Authentisierung

Ein weiterer wichtiger technischer Aspekt ist die gegenseitige Authentisierung der verschiedenen an der Überwachungsmaßnahme verwendeten Systeme. Die DigiTask Software meldet sich mit einem fest einprogrammierten Meldetext, der den vom CCC publizierten Erkenntnissen entspricht. Dies habe ich vor Ort mit Hilfe eines Editors kontrolliert und bestätigt. Dieser Meldetext wird vom Trojaner zum Server geschickt und soll so sicherstellen, dass die richtige Verbindung geknüpft wurde. Durch den fest programmierten Meldetext ist es leicht möglich die Kommunikation beispielsweise in einer Firewall herauszufiltern und umzuleiten. Ich habe keine Hinweise darauf gefunden, dass bei den vom BKA durchgeführten Verfahren über den Abgleich dieses Meldetexts hinaus eine Authentisierung stattgefunden hat.

f) Benutzerverwaltung (Record-Unit-System)

Die in den Räumlichkeiten des BKA betriebene „Record-Unit" (RU - eine Komponente des von der Firma DigiTask bezogenen Systems) empfängt und verwaltet die ausgeleitete Kommunikation. Außerdem dokumentiert das die RU die durchgeführten Programm-Updates. Die RU ist auf einem Server installiert, der in einem kleineren Serverraum untergebracht ist. Zugang haben nur die Administratoren über einen Administrations-PC, der in einem verschlossenen Büro untergebracht ist.

Das System verfügt über eine Benutzerverwaltung. Jeder Nutzer hat eine eigene Kennung und ein Passwort, mit dem er sich gegenüber dem System authentisiert. Nach der Authentisierung kann er auf die ihm zugeordneten Daten und Programme entsprechend der eingeräumten Rechte zugreifen. Grundsätzlich wird zwischen zwei Rollen unterschieden: Administrator und Auswerter. Die Rolle Auswerter kann jeder einzelnen Quellen-TKÜ-Maßnahme zugeordnet werden.

Nur Administratoren haben physisch direkten Zugang zum RU-System. Auswerter können nur über das BKA-eigene Bürokommunikationsnetz auf die RU zugreifen. Zum Zeitpunkt der Kontrolle waren zusätzlich noch zwei besondere Nutzerrollen eingetragen: Dolmetscher und Datenschutz. Beide Kennungen waren nicht personalisiert. Die Datenschutzkennung sei nur für den BfDI eingerichtet worden. Die Kennung Dolmetscher wird von verschiedenen Übersetzern genutzt, die ausgeleitete Gespräche übersetzen sollen.

Grundsätzlich können nur Administratoren Updates ausschließlich von dem direkt am Recording-Unit-Rechner angebundenen Administrations-System auf das Zielsystem

übertragen. Updates werden innerhalb der RU dokumentiert. Die entsprechenden Versionen der Software auf dem Zielsystem werden im BKA für Revisions- und Beweiszwecke vorgehalten.

g) Dokumentation von Updates

Das BKA kann neue bzw. geänderte Überwachungssoftware nur über die Record-Unit auf den Zielrechner aufspielen. Hierzu stellt der zuständige Administrator die entsprechende Updatedatei auf dem RU-Arbeitsplatz bereit und ordnet sie mit der Nachladefunktion dem Zielrechner anhand dessen U-Nummer oder seiner MAC-Adresse zu. Sobald der Zielrechner „online" ist, wird die Nachladefunktion aktiv und führt das Update durch. Bei dem Softwareupdate wird auf der RU auch ein Hash-Wert der übermittelten Software gespeichert (erzeugt wird ein MD5-Hash)[6]. Nach Aussage der zuständigen Mitarbeiter werden von der Capture-Unit gespeichert:

- die aufgespielte Software-Version, die von DigiTask bezogen wurde, und
- alle beim Zielrechner später eingespielten Versionen.

Gespeichert werden dabei die IP-Adresse und die Fall-Nummer. Bei der ersten Lieferung übermittelt DigiTask die Capture-Unit zusammen mit einer Text-Datei, welche den Hash-Wert und eine Beschreibung der Fähigkeiten der Software beinhaltet. Somit ist dokumentiert, welche Fähigkeiten – nach Angaben von DigiTask – die Capture-Unit beinhaltet.

Der Hash-Wert der übermittelten Capture-Unit wird in der Datenbank der RU für jeden Fall (U-Nummer bzw. Mac-Adresse) gespeichert. Eine Änderung ist grundsätzlich denkbar, da die Administratoren Root-Rechte auf der RU haben. Mangels Dokumentation dürfte dies jedoch einen erheblichen Aufwand erfordern. Die verwendete Hash-Funktion, MD5, gilt allerdings als veraltet.[7]

---

[6] Bei einem Hash-Code handelt es sich um einen mit einer bestimmten Funktion (Hash-Funktion) aus einer Datei erzeugten Kontroll-Wert, der die Integrität der jeweiligen Datei gewährleisten soll. Soweit sich der Hash-Code auf eine Programmdatei bezieht, kann damit auch die jeweilige Programmversion identifiziert werden. MD5 ist ein kryptographischer Hash-Algorithmus.

[7] Vgl. Mitteilung des BSI vom 8. 1. 2009, https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2009/080109x509zert.html;jsessionid=5A9F4B94DBC1F29FB90277999500BF82.2_cid251

h) Darstellung für die Auswerter

Die Auswerter erhalten – gesichert durch einen Webserver, der eine Trennung der Netze ermöglicht – Zugriff auf die Oberfläche der Recording-Unit (RU). In der RU wird für jede Online-Session des Zielrechners ein Protokolleintrag erzeugt. Dieser enthält die IP-Adresse des Zielrechners, die Nutzungs- bzw. Verkehrsdaten der Kommunikationssoftware und die mittels der Kommunikationssoftware übermittelten Inhalte.

i) Protokollierung im Recording-Unit System und sonstige Protokollierung

In der RU werden Protokolle (Log-Files) auf Betriebssystemebene (Linux) und von der Datenbank gespeichert. Dadurch werden zwar praktisch alle Aktivitäten der Nutzer mitprotokolliert. Allerdings fehlen eine effektive Auswertemöglichkeit der Protokolle und eine umfassend Dokumentation der Protokollfunktionen. Ebenfalls ist nicht erkennbar, dass Maßnahmen gegen eine Veränderung der aufgezeichneten Protokolle durch den Administrator getroffen wurden.

Es wird, wie oben erwähnt, ein elektronisches Tagebuch geführt, in dem die Administratoren alle Tätigkeiten zu notieren haben. Somit werden Einträge in der RU nachvollziehbar, insbesondere weshalb Tätigkeiten durchgeführt wurden. Dies dient auch intern dazu, die Aktionen eines abwesenden Administrators zu verstehen. Bei einer Stichprobe konnte festgestellt werden, dass Tätigkeiten im Tagebuch eingetragen waren.

j) Aufzeichnung von Raumgesprächen

Ich habe die Funktionsweise der Quellen-TKÜ-Software mit Skype kurz getestet. Hinweise darauf, dass die Überwachungssoftware zur Überwachung von Raumgesprächen bei nicht aktiver Skype-Kommunikation erfolgen kann, haben sich bei der Prüfung nicht ergeben.

k) Kernbereich privater Lebensgestaltung (technische Löschung)

Die RU speichert die ausgeleiteten Gespräche jeweils in einer Datei. Teile des Gespräches, soweit sie den Kernbereich privater Lebensführung betreffen, können nicht gelöscht werden. Es kann immer nur das gesamt Gespräch gelöscht werden. Anhänge, beispielsweise Bilder die während des Gespräches übertragen wurden sind

löschbar. Beim Löschen von Gesprächen und übertragener Dateien werden in den Session Löschvermerke angebracht. Ebenso ist die Löschung einer Session möglich, die ebenfalls dokumentiert wird (vgl. I.6).

l) Löschung der Quellen-TKÜ-Software

Die zur Quellen-TKÜ auf dem Zielrechner aufgebrachte Software – einschließlich der Nachlade-Software - muss bei Beendigung der Maßnahme gelöscht werden. Dies erfolgt nach Aussage des BKA entweder durch Absetzen eines Löschbefehls über den Administratorrechner oder durch physischen Zugriff auf das überwachte System, etwa wenn der Zielrechner bei einer Durchsuchungsmaßnahme sichergestellt worden sei. In diesem Fall erfolge die Löschung der Software, bevor weitere Maßnahmen zur Beweissicherung durchgeführt werden, insbesondere bevor ein Abbild der Festplatte zur Auswertung für forensische Zwecke kopiert wird.

m) Löschung der aufgezeichneten Daten

Auf der Recording-Unit waren zum Zeitpunkt meines Kontrollbesuchs noch Daten und Programme einer größeren Anzahl von Maßnahmen gespeichert. Technisch ist laut BKA die Löschung der Daten einzelner Maßnahmen möglich. Es ist jedoch nicht möglich, sämtliche Inhalte der Kommunikation zu löschen, und dabei eine Feststellung der erhobenen Daten beizubehalten, sofern der Überwachte in Skype die Chat-Funktion nutzte. Die Chats werden als Texte in den Sessions-Protokollen gespeichert.. Eine automatisierte Löschung ist nicht vorgesehen.

In einem Gefahrenabwehrvorgang gemäß § 4a BKAG waren die Daten bereits löschungsreif, wurden allerdings im Hinblick auf die vom mir angekündigte Kontrolle und eine mögliche gerichtliche Überprüfung lediglich gesperrt.

2. ZKA/Zollfahndungsdienst

a) Unterschiede bei der Vorgehensweise von BKA und ZKA

Während das BKA zunächst eine Version der Quellen-TKÜ-Software ohne Überwachungsfunktion aufbringt und diese dann mittels der Nachladefunktion ersetzt, wird vom ZKA direkt eine Software mit Überwachungsfunktion auf den Zielrechner einge-

spielt. Nach Aussage des ZKA wurde die – auch hier vorhandene - Nachladefunktion dort noch nie genutzt.

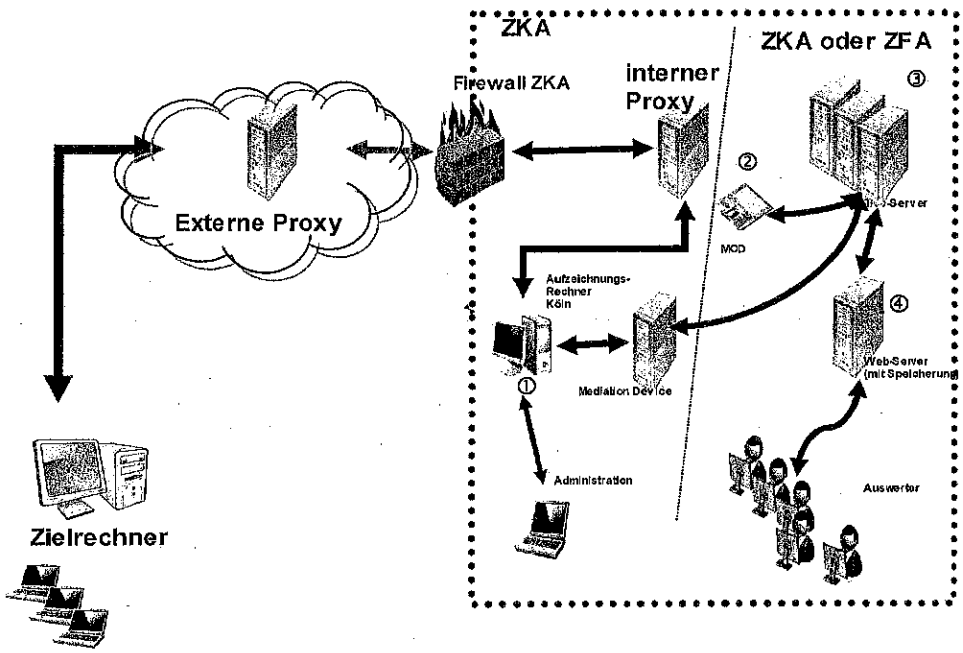
b) TK-Anlage von DigiTask beim ZKA

Die Funktionsweise des vom ZKA verwendeten Verfahrens ist im übrigen – soweit erkennbar – identisch mit dem BKA. Während vom BKA eine Weboberfläche verwendet wird, die von der RU zur Verfügung gestellt wird, nutzt das ZKA die (vorhandene) TKÜ-Infrastruktur. Dazu werden die bei der Quellen-TKÜ aufgezeichneten digitalen Daten über ein Mediation Device (von der Firma DigiTask geliefert) in ein Format gewandelt, welches die TKÜ-Infrastruktur des ZKA verarbeiten kann.

Die umgewandelten Daten werden in einen TKÜ-Aufzeichnungs-Server übermittelt und dort gespeichert. Ferner werden die Daten zur Beweissicherung auf einer Magneto-Optical-Disk (MOD) gespeichert. Da die Daten auf den TKÜ-Aufzeichnungs-Servern in einem Rohformat gespeichert werden, werden sie auf einen „Web-Server" mit Auswertungsfunktion überspielt und dort ebenfalls aufgezeichnet. Somit werden Daten an vier Stellen gespeichert, siehe Systeme ①-④ in der Grafik unten. Die Auswerter greifen auf diesen „Web-Server" zu.
Die mittels Quellen-TKÜ erhobenen Inhalte für die Auswerter werden in einer anderen Weise als beim BKA dargestellt. Dabei werden die Gesprächsinhalte, die übertragenen Dateien und der Inhalt von Chats jeweils in einer separaten Baumstruktur angeordnet. Die IP-Adresse des überwachten Rechners ist nicht mehr erkennbar. Somit kann der Auswerter selbst nicht feststellen, ob der überwachte Rechner am zu überwachenden DSL-Anschluss mit dem Internet verbunden ist bzw. war oder ob er einem anderen Internet-Anschluss, ggf. sogar im Ausland, verbunden ist bzw. war.

Eine Löschung einzelner Gespräche – etwa aufgrund dem Kernbereich zuzuordnender Inhalte – ist nach Angaben des ZKA auf dem „WEB-Server" und der RU durch die jeweiligen Administratoren möglich. Eine Löschung einzelner Gespräche auf der MOD oder dem TKÜ-Server ist dagegen nicht vorgesehen. Auch das Löschen von bestimmten dem Kernbereich zuzurechnenden Gesprächsteilen ist nicht möglich. In der Vergangenheit wurden die Maßnahmen von den ZFÄ selbstständig durchgeführt. Dort und beim ZKA wurde der Aufzeichnungsrechner anfangs nur für jeweils eine Maßnahme gemietet. Aus wirtschaftlichen Gründen wurde dieser Rechner mit der entsprechenden Software nun dauerhaft vom ZKA erworben. Die nun vorhandene Infrastruktur kann so verwendet werden, dass die Infrastruktur bis zum Mediation-Device vom ZKA betrieben wird. Die von DigiTask gelieferte TKÜ-Infrastruktur ist auch bei den ZFÄ in gleicher oder ähnlicher Weise vorhanden. Über verschlüsselte

Verbindungen kann auch die TKÜ-Infrastruktur eines ZFA an das Mediation-Device des ZKA angebunden werden.



c) Dokumentation der DigiTask Software beim ZKA

Das ZKA hält die Versionen der von der Firma DigiTask bezogenen und für Überwachungsmaßnahmen verwendeten Software (Client-Software, Überwachungsprogramme) nicht vor. Es hat die jeweils verwendete Software nach dem Aufspielen auf das Zielsystem gelöscht. Auch Kopien der von DigiTask bezogenen Software waren zum Zeitpunkt meiner Kontrollen beim ZKA nicht mehr vorhanden.
Eine Dokumentation der eingesetzten Programme und Systeme lag nicht vor. Auch der Quellcode wurde von DigiTask nicht bereitgestellt. Daher konnte ich die vom ZKA verwendete Software und die im einzelnen von ihr bereitgestellten und genutzten Funktionalitäten nicht prüfen.

Nach Auskunft des ZKA wird die Versionskontrolle der jeweils eingesetzten Software nicht durch das Amt sondern durch die Firma DigiTask mit Hilfe einer Hashfunktion (SHA-1) vorgenommen. Die Hashwerte der verwendeten Software-Version werden in der RU dokumentiert. Da die Original-Software im ZKA nicht mehr vorhanden ist, war es mir nicht möglich, die tatsächlichen Überwachungsvorgänge und die dabei verwendete Software nachzuvollziehen. Eine beliebige „Original-Software" könnte deshalb nur über den Hashwert wieder identifiziert werden.

Hinsichtlich der Funktionalität und der technischen Einzelheiten der jeweils verwendeten Programme vertraute das ZKA allein den Aussagen von DigiTask. Eigene nachvollziehbare Untersuchungen des ZKA hinsichtlich der Software fanden nicht statt. Nach Mitteilung des ZKA wurde zwar getestet, ob die von DigiTask gelieferte Software die bestellten Funktionalitäten erfüllte. Eine Testung auf eventuelle Programmfunktionalitäten außerhalb der Quellen-TKÜ fand nicht statt.

Das ZKA verfügte zum Zeitpunkt meines Prüfungsbesuchs über kein Sicherheitskonzept für die Durchführung von Maßnahmen der Quellen-TKÜ. Ein Sicherheitskonzept über die Infrastruktur ist nach Auskunft des ZKA derzeit aber in der Bearbeitung.

d) Proxy Server beim ZKA

Die IP-Adresse des für die Steuerung des Ladeprogramms und der Überwachungssoftware eingesetzten Servers („Command-and-Control-Server") war – wie diejenige des bei den Quellen-TKÜ des BKA eingesetzten Servers - frei konfigurierbar. Der Server war zum Zeitpunkt meines Kontrollbesuchs nicht mehr aktiv und erreichbar. Ein weiterer externer Proxy wurde an einem anderen Standort betrieben. Die beiden Server wurden vom ZKA angemietet und standen unter seiner Kontrolle.

Die Proxy-Server arbeiten mit dem Betriebssystem Linux. Eine von der Firma DigiTask gelieferte ausführbare Datei muss auf dem Linux-System installiert und konfiguriert werden. Insbesondere wird festgelegt, ob und für welche Server dynamische IP-Adressen verwendet werden. Die ausführbare Datei wurde von DigiTask ohne Quellcode geliefert, so dass auch hier auf die Firma vertraut werden musste.

Auf den Proxy-Servern werden Log-Files geschrieben, in dem Verbindungen protokolliert werden. Auf einem Proxy wird auch die IP-Adresse der überwachten Rechner protokolliert, so dass ein potentieller Angreifer auch im Nachhinein Hinweise auf das überwachte System erhalten könnte. Allerdings wurden eventuelle Angriffsversuche auf den Server protokolliert.

e) ERA-Software beim ZKA

In einigen länger zurückliegenden Fällen wurde die Software der Schweizer Firma ERA IT Solutions AG genutzt. Die Weiterentwicklung der Software wurde 2008 eingestellt. Beim Besuch wies das ZKA darauf hin, dass insoweit alle Maßnahmen von den ZFA durchgeführt wurden und somit keine Erkenntnisse beim ZKA vorliegen. Da

einige der überlassenen Unterlagen der ERA IT Solutions AG an das ZKA adressiert sind, ist diese Aussage nicht nachvollziehbar.

Die ERA-Software unterscheidet sich von dem DigiTask-Produkt in einigen Punkten. Im Hinblick darauf, dass diese Software bereits seit längerer Zeit nicht mehr vom ZKA verwendet wird, wird hier von einer näheren Betrachtung abgesehen.

C. Bewertung

Die vom BKA, der Bundespolizei, dem ZKA bzw. den ZFÄ durchgeführten Maßnahmen der Quellen-TKÜ kann ich datenschutzrechtlich nur eingeschränkt bewerten, da meiner vollständigen Kontrolle teilweise rechtliche Hindernisse entgegenstehen. Dies gilt zum einen insoweit, als diese Behörden gerichtliche Beschlüsse durchgeführt haben (I.1.). Denn ich bin insoweit an die Wirkung der gerichtlichen Entscheidungen gebunden, auch wenn ich teilweise andere Rechtsansichten vertrete (I.2.). Zum anderen gilt dies insoweit, als das BKA, die Bundespolizei, das ZKA bzw. die ZFÄ bei der Durchführung strafrechtlicher Ermittlungen auf Weisung einer jeweils zuständigen Staatsanwaltschaft eines Landes gehandelt haben, die nur der datenschutzrechtlichen Kontrolle der nach dem jeweiligen Landesrecht zuständigen Stelle unterworfen ist. Soweit es die jeweilige Durchführung der Maßnahme in der Verantwortung der genannten Behörden liegt, bewerte ich im Folgenden die festgestellten Sachverhalte (II.):

I. Rechtsgrundlage für die Durchführung der Quellen-TKÜ

1. Vorliegende gerichtliche Beschlüsse

Zu allen durchgeführten Maßnahmen der genannten Behörden lagen gerichtliche Beschlüsse vor, die sie jeweils dazu ermächtigt haben, eine Quellen-TKÜ gegen die betroffenen Personen durchzuführen. Damit ist festzustellen, dass die Durchführung der Maßnahmen als solche dem Grunde nach durchweg datenschutzrechtlich zulässig war.

Die Maßnahmen wurden, soweit sie strafrechtliche Ermittlungsverfahren betrafen, auf § 100a der StPO gestützt. Maßnahmen der Gefahrenabwehr wurden vom BKA auf der Grundlage der §§ 20k, 20l BKAG, seitens des ZKA auf der Grundlage der §§ 23a ff. ZFdG durchgeführt.

Eine eigene datenschutzrechtliche Bewertung, ob im jeweiligen Einzelfall die Anordnungsvoraussetzungen der § 100a StPO, §§ 20k, 20l BKAG bzw. 23a ff. ZFdG vorgelegen haben, ist mir aus Respekt vor der richterlichen Unabhängigkeit verwehrt. Unmittelbar ergibt sich dies aus § 24 Abs. 3 Bundesdatenschutzgesetz (BDSG), wonach die Bundesgerichte nicht meiner Kontrolle unterliegen, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Für die Gerichte der Länder ergibt sich dies

schon daraus, dass ich für die Kontrolle von Landesbehörden nicht zuständig bin, darüber hinaus aus Art. 97 GG.

2. Datenschutzpolitische Bewertung

Insofern habe ich mich, außerhalb der konkreten Einzelfälle, darauf zu beschränken, in allgemeiner Form auf meine grundsätzlichen Zweifel hinzuweisen, ob § 100a StPO sowie § 23a ZFdG als hinreichende Rechtsgrundlagen für eine Quellen-Telekommunikationsüberwachung tragfähig sind:

Das Bundesverfassungsgericht hat auf die besonderen Risiken hingewiesen, die mit einer Quellen-Telekommunikationsüberwachung verbunden sind.[8] Mit der Infiltration des Systems sei „die entscheidende Hürde genommen, um das System insgesamt auszuspähen."[9] Diese Gefahren allerdings entstehen nicht nur durch das gezielte Auslesen des Systems durch Ermittlungsbehörden, sondern auch durch abstrakte Gefährdungen. Diese können entstehen, wenn eine Behörde Sicherheitslücken des betroffenen Systems gezielt ausnutzt und eine Überwachungssoftware einfügt. Eine abstrakte Gefährdung über die konkrete Ermittlungstätigkeit der Behörde hinaus entsteht etwa dann, wenn die Infiltration es – auch unabsichtlich – Dritten ermöglicht, in das System einzudringen (beispielsweise durch eine unzureichende Authentifizierung und Verschlüsselung, durch die es einem unberechtigten Dritten ermöglicht wird, eine Nachladefunktion zu nutzen). Zudem besteht das Risiko, dass unbeabsichtigt Informationen ohne Bezug zur laufenden Telekommunikation erhoben werden. Diese können zum Beispiel den Zustand des eingeschalteten Endgeräts betreffen. Das Bundesverfassungsgericht hat damit nicht allein auf die gezielte Erfassung von Informationen abgestellt. Für relevant hielt es bereits „das Risiko, dass über die Inhalte und Umstände der Telekommunikation hinaus weitere persönlichkeitsrelevante Informationen erhoben werden."

Das Gericht hat entschieden, dass Art. 10 GG als alleiniger grundrechtlicher Maßstab für die Beurteilung einer Ermächtigung zu einer Quellen-Telekommunikationsüberwachung ausreichend sei, wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränke.[10] Hieraus folgt aber lediglich, dass insoweit das – wesentlich höhere Eingriffsschwellen verlangende – Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme nicht als Eingriffsmaßstab heranzuziehen ist.

---

[8] BVerfG NJW 2008, 822, 825, Abs. Nr. 188
[9] BVerfG a.a.O.
[10] BVerfG a.a.O.

Aus dieser Aussage des Bundesverfassungsgerichts kann jedoch nicht geschlossen werden, dass insoweit eine besondere gesetzliche Regelung nicht erforderlich sei. Im Gegenteil: Es genügt nicht, Maßnahmen der Quellen-Telekommunikationsüberwachung lediglich in der Praxis zu beschränken. Das Bundesverfassungsgericht fordert neben technischen Vorkehrungen ausdrücklich „rechtliche Vorgaben", die den mit der Infiltration des Systems verbundenen Eingriff auf die Überwachung der Telekommunikation beschränken.[11] Damit kann nichts anderes gemeint sein als eine hinreichend normenklare und bestimmte Rechtsgrundlage.[12] Diese muss insbesondere die geforderten technischen Beschränkungen ausdrücklich regeln, die sicherstellen, dass sich die Überwachung auf Telekommunikationsinhalte beschränkt. Bereits aus dem Vergleich des § 100a StPO mit den neueren § 20l Abs. 2 i.V.m. § 20k BKAG, die ausdrücklich die Quellen-Telekommunikationsüberwachung regeln, zeigt sich, dass die Strafprozessordnung solche Vorgaben nicht enthält.[13] Solche Vorgaben ergeben sich auch nicht aus § 100b Abs. 2 Satz 2 Nr. 3 StPO, der die Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt;[14] denn anders als § 20k Abs. 2 und 3 BKAG, auf den in § 20l Abs. 2 BKAG verwiesen wird, ergeben sich aus der strafprozessualen Vorschrift keine besonderen technischen und verfahrensmäßigen Sicherungen.

Das Regelungssystem der §§ 100a und 100b StPO ist vielmehr auf das Zusammenspiel mit den Vorschriften der Telekommunikations-Überwachungsverordnung (TKÜV) abgestimmt. Diese ist gemäß § 3 Abs. 1 TKÜV aber nur anwendbar, wenn an der Überwachung Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, mitwirken. Dies ist bei der Quellen-TKÜ aber nicht der Fall. Damit sind wesentliche gesetzliche Vorgaben zum Verfahren, zur Ausleitung der überwachten Gespräche und zur Übermittlung an die jeweilige Behörde (§§ 6 ff. TKÜV) sowie zur Protokollierung (§§ 16 f. TKÜV) nicht anwendbar. Hierbei handelt es sich um technische Verfahrensregeln, die sicherstellen sollen, dass die Überwachung auch in technischer Hinsicht auf das rechtlich zulässige Maß beschränkt bleibt. Diese sind für die verfahrensmäßige Abfederung des Grundrechtseingriffs unabdingbar.

Ebenso stellt sich die Frage, ob eine Quellen-TKÜ mit den Regelungen in § 100b Abs. 2 Satz 2 Nr. 2, Abs. 3 StPO kompatibel ist, wenn weder das Endgerät genau benannt noch technisch sichergestellt werden kann, dass nur die über einen bestimmten Anschluss geführte Kommunikation überwacht wird.

---

[11] BVerfG a.a.O.
[12] Braun/Roggenkamp K&R 2011, 681, 683; Buermeyer/Bäcker HRRS 2009, 433, 438.
[13] vgl. Klesczewski ZStW 2011, 737, 743 m.w.N.
[14] Buermeyer/Bäcker HRRS 2009, 433, 438.

3. Installation der Überwachungssoftware

Eine weitere Frage ist, wie der Eingriff in das Zielsystem durch die Installation der Überwachungssoftware zu bewerten ist. Zu Recht wird in der Literatur darauf hingewiesen, dass die Infiltration ein eigenständiger Eingriff in das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme ist.[15] Da die Installation aber von den gerichtlichen Beschlüssen dem Grunde nach vorausgesetzt wird, enthalte ich mich einer datenschutzrechtlichen Bewertung.

Keine Aussagen habe ich in den Tenorierungen allerdings dazu gefunden, dass die Überwachungssoftware nicht nur „von Ferne" (z.B. durch E-Mail), sondern durch die Manipulation sichergestellter Asservate erfolgen darf. Insoweit ist der Sachverhalt einer datenschutzrechtlichen Bewertung zugänglich.

Das heimliche Betreten von Wohnungen zur Installation der Überwachungssoftware würde von vornherein gegen den Grundsatz der Offenheit der Wohnungsdurchsuchung verstoßen und wäre daher mit Art. 13 Abs. 2 GG unvereinbar.[16] Einen derartigen Fall habe ich aber nicht vorgefunden.

Allerdings stellt sich die Frage, ob sich eine ähnliche Bewertung ergibt, wenn ein bei einer offenen Maßnahme beschlagnahmtes Asservat heimlich manipuliert wird. Dies ist zu bejahen, da die strafprozessualen Vorschriften der Durchsuchung und Beschlagnahme insoweit nur die Durchsicht, ggf. die Sicherung von Schriftstücken und elektronischen Speichermedien gestatten (§ 110 StPO) bzw. die Verwendung als Beweismittel (§ 94 Abs. 1 StPO). Die Regelung des § 110 StPO enthält zudem Restriktionen über den Kreis der zur Durchsicht befugten Beamten. Die Manipulation ist daher von den Vorschriften über die Beschlagnahme und Durchsuchung nicht gedeckt. Die heimliche Manipulation würde darüber hinaus mittelbar gegen den Grundsatz der Offenheit nach Art. 13 Abs. 2 GG verstoßen. § 110 Abs. 2 Satz 2 StPO zeigt, dass auch die Regelungen zur Durchsicht beschlagnahmter Papiere bzw. Speichermedien vom Grundsatz der Offenheit geprägt sind.

II. Art der Durchführung

Die nachfolgenden Ausführungen gelten im Wesentlichen für Maßnahmen des BKA und des Zollfahndungsdienstes. Die Quellen-TKÜ-Maßnahme im Rahmen der von der Bundespolizeidirektion München geführten Ermittlungsverfahrens wurde in

---

[15] Buermeyer, Bäcker, HRRS 2009, 433, 439; Braun K&R 2011, 681, 684.
[16] Braun a.a.O. m.w.N.

Amtshilfe durch das Bayerische Landeskriminalamt (BLKA) durchgeführt. Einzelheiten hierzu liegen mir nicht vor. Die diesbezügliche Prüfung des Bayerischen Landesbeauftragten für den Datenschutz dauern an.

1. Rechtliche Anforderungen an die Datensicherheit

Die rechtlichen Anforderungen an die Datensicherheit stellen sich wie folgt dar:

Das Bundesverfassungsgericht hat – bezogen auf die Quellen-TKÜ – die Infiltration des Zielcomputers als „die entscheidende Hürde" angesehen, „um das System insgesamt auszuspähen".[17] Damit hat es die mit jeder Infiltration verbundene abstrakte Gefährdung, beispielsweise durch unabsichtliche Datenverluste oder einen Missbrauch der verwendeten Software durch Dritte, herausgestellt[18] (siehe dazu auch oben I.2.). Aus dieser spezifischen Gefährdungslage resultieren besondere Anforderungen an die Datensicherheit und die Protokollierung, die über die allgemeinen Anforderungen an die Datensicherheit hinausgehen.

Dementsprechend hat der Gesetzgeber für Maßnahmen des BKA zur Gefahrenabwehr besondere Regelungen in § 20l Abs. 2 Satz 2 i.V.m. § 20k Abs. 3 BKAG verankert. Gemäß § 37 BKAG, § 37 BPolG bzw. § 43 ZFdG ist jeweils ergänzend § 9 BDSG anzuwenden.

Wie oben unter I.2.. ausgeführt, fehlen entsprechende Spezialregelungen für den Bereich der strafprozessualen Telekommunikationsüberwachung nach § 100a StPO bzw. § 23a ZFdG, die die Quellen-TKÜ nicht erfassen. Das BKA hat allerdings vorgetragen, die Eingrenzungen der §§ 20k Abs. 2 und Abs. 3, 20l Abs. 2 BKAG entsprechend anzuwenden. M. E. haben die weitergehenden Anforderungen des BKAG bis zu einer entsprechenden Änderung der §§ 100a, 100b StPO bzw. der §§ 23a ZFdG bei allen Maßnahmen der Quellen-TKÜ durch Polizeibehörden des Bundes zu gelten. Dies folgt auch aus den Vorgaben, die das Bundesverfassungsgericht u.a. in seiner Entscheidung zur sog. Online-Durchsuchung[19] herausgestellt hat.

Weitere Anforderungen an die Datensicherheit ergeben sich aus der Frage, welcher Beweiswert den mittels Online-Zugriffen erhobenen Daten zukommen kann. § 9 BDSG soll als verfahrenssichernde Vorschrift den Grundrechtseingriff abfedern. Insofern sind die Anforderungen umso höher, als die möglichen Folgen des Grundrechtseingriffs für den Betroffenen besonders schwerwiegend sind. Dies ist insbe-

[17] BVerfG NJW 2008, 822, 825 f.
[18] vgl. BVerfG a.a.O.,
[19] BVerfG NJW 2008, 822.

sondere der Fall, wenn erlangte Daten zumindest potentiell als Beweismittel gegen ihn eingesetzt werden können. Das Bundesverfassungsgericht hat in Betracht gezogen, dass der Beweiswert von Informationen, die mittels Online-Zugriff auf ein informationstechnisches System erhoben wurden, möglicherweise begrenzt sein kann, weil eine technische Echtheitsbestätigung der erhobenen Daten grundsätzlich eine – hier nicht vorhandene – exklusive Kontrolle des Zielsystems voraussetzt.[20] Es hat allerdings konstatiert, dass den Daten deshalb nicht der Informationswert abgesprochen werden kann. Für das Gericht war im Zusammenhang mit dem von ihm zu entscheidenden Sachverhalt – der Regelung eines Landesverfassungsschutzgesetzes – maßgebend, dass die Verfassungsschutzbehörden Informationen zur Prävention im Vorfeld konkreter Gefahren nicht mit derselben Beweissicherheit erheben müssen, wie dies für die Strafverfolgungsbehörden in einem Strafverfahren gilt. Im Umkehrschluss ergeben sich für die hier in Rede stehenden strafprozessualen Maßnahmen besonders hohe Anforderungen an die Authentizität der als Beweismittel aufgezeichneten Telekommunikation.
Dagegen kann nicht eingewandt werden, dass insoweit für die Quellen-TKÜ – in Abgrenzung zur sonstigen sog. Online-Durchsuchung – geringere Anforderungen gelten würden. Denn technisch gesehen wird beides mit denselben Methoden durchgeführt. Geringere Anforderungen bei der Quellen-TKÜ gelten auch nicht deshalb, weil die Gesprächsinhalte oder die aufgezeichneten Stimmen konkreten Personen zuzuordnen sein könnten. Denn dies würde die technischen Widrigkeiten verkennen, wie sie für die Telekommunikationsüberwachung nach Auffassung des Bundesverfassungsgerichts offenbar recht allgemein gelten. Denn die bei der Telekommunikationsüberwachung aufgezeichneten Gespräche sind „auch aus sonstigen, der Nutzung des Mediums geschuldeten Gründen wie zum Beispiel Hintergrundrauschen oder schlechter Empfang kaum ohne technische Aufbereitung beim ersten Hören zu verstehen (vgl. BT-Drucks 16/5846, S. 44)."[21]

Allerdings gilt für die Quellen-TKÜ die – im Vergleich zur Online-Durchsuchung - zusätzliche Anforderung, dass die Überwachung technisch auf die laufende Telekommunikation zu begrenzen ist.

Jede Sicherheitsbehörde hat demnach unabhängig von der Rechtsgrundlage, auf die sie sich bei der Quellen-TKÜ stützt, hinsichtlich der Datensicherheit mindestens folgendes zu beachten:

---

[20] BVerfG NJW 2008, 822, 829.
[21] BVerfG, Urt. vom 12. Oktober 2011, 2 BvR 236/08, Abs. Nr. 219, www.bundesverfassungsgericht.de.

a) Die Maßnahme kann nur dann als Telekommunikationsüberwachung an Art. 10 GG gemessen werden, wenn sie sich auf die Überwachung der laufenden Telekommunikation bezieht und dies durch rechtliche und technische Vorgaben sichergestellt ist.[22] Dieser verfassungsrechtlichen Vorgabe folgend bestimmt § 20l Abs. 2 Satz 1 Nr. 1 BKAG für den Bereich der Gefahrenabwehr ausdrücklich, dass diese Beschränkung auf die Überwachung der laufenden Kommunikation durch technische Maßnahmen sichergestellt sein muss. Für eine Quellen-TKÜ auf Grundlage des § 100a StPO bzw. § 23a ZFdG ist diese Vorgabe zumindest entsprechend anzuwenden.

b) Gemäß § 20k Abs. 2 Satz 1 BKAG ist technisch sicherzustellen, dass an dem Zielsystem nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind. Zudem muss die Behörde die vorgenommenen Veränderungen soweit technisch möglich automatisiert rückgängig machen können, wenn sie die Maßnahme beendet.

   Die zur Überwachung eingesetzten Mittel sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen, § 20 Abs. 2 Satz 2 BKAG. Diese Regelung trägt dem Umstand Rechnung, dass sich der intensive Grundrechtseingriff bereits mit der Infiltration des Zielsystems und der dadurch veranlassten Ausleitung der Daten vollzieht. Dementsprechend müssen hinsichtlich des verwendeten Gesamtsystems (Zielsystem, Proxys, Arbeitsplatzrechner) technische Vorkehrungen getroffen werden, die sicherstellen, „dass die Software nicht durch Dritte (Hacker) zweckentfremdet werden kann".[23] Als Beispiele nennt die Gesetzesbegründung: Die Software muss darauf begrenzt sein, Inhalte nur an den vom BKA voreingestellten Server auszuleiten. Zudem darf sie nicht von Dritten ansprechbar sein.

c) Werden Daten kopiert, sind diese gemäß § 20 Abs. 2 Satz 3 BKAG nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Diese Regelung schließt damit nahtlos an Satz 2 an und betrifft den gesamten Ausleitungsvorgang („vom Zeitpunkt der Bereitstellung für die Übertragung an das BKA an, während der Datenübertragung an das BKA sowie während ihrer Speicherung beim BKA.") und schützt auch insoweit die „Integrität und Authentizität der von dem technischen Mittel bereitgestellten Daten".[24]

---

[22] BVerfG NJW 2008, 822, 826.
[23] BT-Drs. 16/9588 S. 27.
[24] BT-Drs. 16/9588 a.a.O.

Für den Bereich des mit der Vorratsspeicherung von Telekommunikationsverkehrsdaten verbundenen besonders intensiven Grundrechtseingriffs fordert das Bundesverfassungsgericht u.a. eine asymmetrische kryptographische Verschlüsselung verbunden mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln sowie den Einsatz von automatisierten Fehlerkorrektur- und Plausibilitätsverfahren.[25] Angesichts der Eingriffsintensität und der mit dem Online-Zugriff verbundenen Risiken für die Datensicherheit dürften diese Anforderungen hier übertragbar sein.

d) Der Beweissicherheit und der Gewährleistung effektiven Grundrechtsschutzes dient die Regelung zur Protokollierung.[26]

Gemäß § 20l Abs. 2 Satz 2 i.V.m. § 20k Abs. 3 BKAG sind bei jedem Einsatz des technischen Mittels zu protokollieren:

- die Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes,
- die Angaben zur Identifizierung des informationstechnischen Systems und die daran vorgenommenen nicht nur flüchtigen Veränderungen,
- die Angaben, die die Feststellung der erhobenen Daten ermöglichen und
- die Organisationseinheit, die die Maßnahme durchführt.

e) In den Fällen strafprozessualer Maßnahmen erscheint insofern fraglich, ob die Vorgaben des § 20k Abs. 3 BKAG, der der Gefahrenabwehr dient, eine hinreichend beweissichere Erhebung von Telekommunikationsinhalten vorgeben. Insofern ist neben den vom Bundesverfassungsgericht für den Bereich der Vorratsspeicherung von Telekommunikationsverkehrsdaten aufgezeigten Möglichkeiten einer verbesserten Datensicherheit eine revisionssichere Protokollierung zu fordern.

2. Technische Umsetzung

Die technische Umsetzung der rechtlichen Anforderungen an die Datensicherheit bewerte ich wie folgt:

Die rechtlichen Anforderungen erfordern bei der technischen Umsetzung eine Reihe technischer Maßnahmen, die weit über die Anforderungen an gängige Überwachungssoftware hinaus gehen. Software von Sicherheitsbehörden für Quellen-TKÜ-

[25] vgl. BVerfG NJW 2010, 833, 840.
[26] BT-Drs. 16/9588.

Maßnahmen sollen eben technisch nicht wie Schadsoftware, Viren, Spionageprogramme und Hackerprogramme funktionieren und irgendjemanden ausspionieren können. Sie müssen vielmehr die gesetzlichen Vorgaben und Standards des Datenschutze und der IT-Sicherheit erfüllen. Hierzu gehören Maßnahmen zu Gewährleistung der Transparenz, Vertraulichkeit, Verfügbarkeit und Unversehrtheit, aber auch zu Revisionssicherheit und Löschbarkeit.
Die Transparenz der Software ist deshalb erforderlich, weil sie nur so zuverlässig geprüft werden kann. Insbesondere muss nachprüfbar sein, dass die eingesetzte Technik den rechtlichen Vorgaben entspricht und insbesondere die Überwachung die vorgeschriebenen Grenzen nicht überschreitet.

Auch die Verhältnismäßigkeit des mit der Überwachung verbundenen Grundrechtseingriffs muss gegeben sein. Nicht alles, was technisch machbar ist, darf auch eingesetzt werden. Dem entsprechend müssen die Überwachungsfunktionen so zugeschnitten werden, dass keine unzulässige Informationserhebung stattfindet.

Ob diese Grenzen eingehalten werden, kann nur durch die Begutachtung und systematisches Testen der Software beurteilt werden. Erforderlich ist hierzu die Vorlage des sogenannten Quellcodes - einen lesbaren, in einer Programmiersprache geschriebenen Text der eingesetzten Software -, damit sich die verantwortliche Stelle nachhaltig über den Umfang der zur Verfügung stehenden programmierten Funktionen überzeugen kann. Auch eine verlässliche und umfassende interne oder externe Datenschutzkontrolle ist nur unter diesen Voraussetzungen möglich.

Insbesondere ist ohne die Vorlage des Quellcodes eine sichere Beurteilung einer Software hinsichtlich des Vorhandenseins oder eben Nichtvorhandenseins von Funktionen nicht möglich. Die Übersendung oder Vorlage nur eines umfangreichen ausführbaren Programms (Codes, Binärcodes) reicht zur Beurteilung nicht, denn vor allem das Nichtvorhandensein von Funktionen kann allein anhand eines Binärcodes nicht abschließend bewertet werden.

Auch (mögliche) Seiteneinstiege für Dritte und andere Sicherheitslücken sind allein mit Hilfe des Binärcodes nicht auszuschließen. Gerade bei Überwachungssoftware, mit der in einem rechtstaatlichen Verfahren auch gerichtsverwertbare Daten erhoben werden sollen, sind Fragen nach den Möglichkeiten der Manipulation der Daten von immenser Wichtigkeit. Die Vertraulichkeit und Unversehrtheit der erhobenen Daten sind hier von entscheidender Bedeutung. Dies betrifft nicht nur die Übertragungswege, sondern auch die Speicherung der Daten in jedem Stadium der Überwachungsmaßnahme.

Zudem stellen sich Fragen zur Verfügbarkeit, denn die Software soll ja in einem bestimmten zeitlichen Rahmen Ergebnisse liefern. Die Verfügbarkeit ist auch entscheidend für die Deaktivierung und Deinstallation von Überwachungssoftware und die Löschung von Daten.

Schließlich muss die Revisionssicherheit des Gesamtsystems gewährleistet sein. Nicht nur die Software muss umfassend dokumentiert werden, sondern auch die Bedingungen ihres Einsatzes einschließlich aller beteiligten Systeme.

Während des gesamten Prozesses müssen die Daten vertraulich, zuverlässig und unversehrt verarbeitet werden. Dies muss das jeweilige Verfahren garantieren können. Zwei Anforderungen spielen dabei eine besondere Rolle: Vertraulichkeit und Authentisierung. Das Verfahren muss deshalb besonderen Wert auf diese beiden Anforderungen legen, weil die Software heimlich aufgebracht wird und auch ihr Betrieb heimlich erfolgt. Es liegt in der Natur der Sache, dass eine derartige Überwachungsmaßnahme die Mitwirkung des Betroffenen bei allen Vorgängen nicht vorsieht oder gar mit einbezieht. Der Betroffenen soll gerade von der Überwachungsmaßnahme nichts erfahren und erkennen können.

Das heimliche Einschleusen von Software bedeutet letztendlich auch, dass sichergestellt sein muss, dass die Daten auf dem Weg zur Sicherheitsbehörde nicht verändert oder verfälscht werden können und das der Empfänger sicher sein kann, dass die Daten vom Rechner des Betroffenen sind und von keiner anderen Person stammen können. Im technischen Sinn ergeben sich daraus strenge Anforderungen an die Daten- und Instanzauthentisierung.

Unter Datenauthentisierung werden (kryptographische) Verfahren verstanden, die garantieren, dass übersandte und/oder gespeicherte Daten nicht verändert wurden und/oder verändert werden können. Unter Instanzauthentisierung werden (kryptographische) Protokolle verstanden, in denen ein Empfänger einem Sender den Besitz eines Geheimnisses nachweist. Bei symmetrischen Verfahren ist dies ein symmetrischer Schlüssel, um seine Identität zu beweisen. Sowohl die Daten- als auch die Instanzauthentisierung erfolgt meist gegenseitig und geht mit einer Schlüsseleinigung einher, um die Vertraulichkeit und Integrität zu gewährleisten. Solche Authentisierungen sichern letztendlich Glaubwürdigkeit und Richtigkeit der Daten und sind deshalb unter den rechtlichen Voraussetzungen unabdingbar.

Heimlichkeit impliziert aber auch die Unbeobachtbarkeit der Überwachungsmaßnahme selbst. Nur, wenn die Überwachungsmaßnahme selbst unbeobachtet ist, ist sichergestellt, dass keine Dritten Einfluss auf die Maßnahme nehmen können. Die

hohen Anforderungen an die Heimlichkeit hat eben auch Folgen für die Anforderungen an die Daten- und Instanzauthentisierung. Wenn alles heimlich und verdeckt erfolgen muss, muss sichergestellt sein, dass die Kommunikationspartner sich richtig identifizieren und dass die Daten unversehrt und vertraulich weitergereicht und gespeichert werden.

Nach dem Ende der Maßnahme muss sichergestellt werden, dass einerseits die Programme nicht weitergenutzt werden können und anderseits auch keine Weiterverbreitung der Überwachungssoftware möglich ist, d.h. die Löschbarkeit der Software ist wichtig. Die Programme müssen Mechanismen enthalten, die eine datenschutzgerechte Löschung des Programmcodes und aller veränderten Parameter gewährleisten. Dies gilt auch für die erhobenen Daten – auch sie müssen effektiv und nicht wiederherstellbar gelöscht werden.

Da aufgrund verfassungsrechtlicher und gesetzlicher Vorgaben der Kernbereich privater Lebensgestaltung besonders geschützt ist, muss die für die Maßnahme eingesetzte Software entsprechende Vorgaben erfüllen, und zwar in jeder Phase der Überwachung. Jedenfalls nach Speicherung der Informationen muss eine gezielte Löschung kernbereichsrelevanter Inhalte möglich sein.

Um eine Kontrolle durch den Betroffenen oder eine Datenschutzbehörde zu ermöglichen, ist eine Protokollierung der wichtigsten Rahmenbedingungen und zu den übermittelten Daten erforderlich. § 20l Abs. 2 Satz 2 i. V. m. § 20k Abs. 3 BKAG macht hierzu umfangreiche Vorgaben. Eine solche Protokollierung muss jedoch auch durch die aufzeichnende Software angemessen unterstützt werden.

Unter diesen allgemeinen Vorbemerkungen sind die folgenden Ausführungen zu sehen.

a) Prüfbarkeit des Überwachungssystems

Die Überwachung der Telekommunikation stellt einen erheblichen Eingriff in das durch Art. 10 GG geschützte Fernmeldegeheimnis dar. Dies gilt für Quellen-TKÜ, in besonderem Maße, weil diese eine Infiltration des von einem Beschuldigten verwendeten Computers voraussetzt und damit die Vertraulichkeit und Integrität des informationstechnischen Systems berührt.

Dem sollen die Regelungen im BKA-Gesetzes Rechnung tragen, die für diesen Eingriff besondere technische, organisatorische und rechtliche Anforderungen formulie-

ren. Die bei der Quellen-TKÜ getroffenen technisch-organisatorischen Maßnahmen müssen neben den allgemeinen Anforderungen des Datenschutzrechts (insbesondere § 9 BDSG) auch diesen besonderen Anforderungen entsprechen.

Seit der Novellierung des BDSG zum 01.09.2010 werden gemäß der Anlage zu § 9 Satz 1 BDSG für besonders schützenswerte Daten besondere Maßnahmen gefordert, u.a. die Verschlüsselung nach dem Stand der Technik gefordert. Betroffen hiervon sind insbesondere Maßnahmen nach Ziffer 2 (Zugangskontrolle), Ziffer 3 (Zugriffskontrolle) und Ziffer 4 (Weitergabekontrolle) dieser Anlage. Alle geforderten Maßnahmen sind auch beim Einsatz einer Quellen-TKÜ-Software von entscheidender Bedeutung.

Da sich der Einsatz einer Überwachungssoftware auf dem Rechner des Betroffenen der direkten Administration durch die Behörde entzieht, muss sichergestellt werden, dass

- nur Befugte Zugriff auf die Überwachungssoftware haben,
- die ausgeleiteten Datenströme vertraulich und integer übertragen werden,
- diese Datenströme nur berechtigten Empfängern zugeleitet werden,
- die Steuerung der Überwachungssoftware nur durch Befugte und
- die Löschung nach Beendigung der Überwachung (oder bei fälschlich infizierten Systemen) nachhaltig erfolgt.

An die Sicherstellung dieser Ziele sind wegen der Eingriffstiefe besonders hohe Anforderungen zu stellen.

Die verantwortliche Stelle hat zu gewährleisten, dass die Hard- und Software den Anforderungen an die Rechtmäßigkeit entsprechen und insbesondere die Vollständigkeit, Vertraulichkeit, Unversehrtheit der Daten sicherstellen. Die Umsetzung der Maßnahmen muss korrekt und sicher erfolgen.

So dürfen in der Software keine Funktionen vorhanden sein, die über die gesetzlich vorgeschrieben Überwachungsmaßnahmen hinaus gehen. Speziell muss – wie auch das Bundesverfassungsgericht festgestellt hat[27] (vgl. I.2.) - sichergestellt werden, dass keine über die Überwachung der laufenden Telekommunikation hinausgehende Überwachung stattfindet.

[27] BVerfGE NJW 2008, 822, 826, Abs.Nr. 190.

Eine Software lässt sich prinzipiell dadurch prüfen, dass der Programmcode unter Hinzuziehung der Verfahrensdokumentation analysiert wird. Dies kann durch geeignete Testverfahren unterstützt werden.

Bei Software ist zwischen Quell- und Binärcode zu unterscheiden. Bei dem Quellcode handelt es sich um für Menschen lesbare, in einer Programmiersprache geschriebene Texte eines Computerprogrammes. Der Quellcode wird durch spezielle Software (Compiler und Linker) in vom Computer ausführbaren Binärcode übersetzt. Da letzterer nur aus einer Folge der Werte „0" und „1" besteht, ist es ohne weitere (Software-) Hilfsmittel praktisch nicht möglich, die genaue Funktionsweise von Programmen allein auf Basis des Binärcodes sicher und abschließend zu begutachten.

Nur durch die Prüfung des Quellcodes und die anschließende kontrollierte Generierung des Binärcodes kann sichergestellt werden, dass in der eingesetzten Software keine verborgenen Funktionalitäten vorhanden sind, die beispielsweise einem Dritten (Unbefugten) erlauben könnten, direkt Zugriff auf die auf einem Zielrechner installierte Überwachungssoftware zu nehmen und diese für andere Zwecke zu missbrauchen. Eine „händische" Quellcodeanalyse ist bei umfangreichen Computerprogrammen außergewöhnlich zeitaufwändig. Bei komplexerer Software stößt sie zudem auf kaum zu überwindende Schwierigkeiten. Aus diesem Grund ist es angezeigt, auch für die Analyse von Quellcodes spezielle Software einzusetzen.

Nur durch die Analyse des Quellcodes sichergestellt werden, dass keine Funktionen benutzt oder vorhanden sind, die über das erlaubte und gebotene Maß hinaus die Rechte des Betroffenen beim Einsatz der Software berühren. Alternativen zur Quellcode-Analyse sind nicht ersichtlich.

Tests können zwar sicherstellen, dass die Software bestimmte geforderte Funktionalitäten enthält und dass sie den Anforderungen an ihre Handhabung genügt. Allein durch Testläufe ist aber nicht auszuschließen, dass eine Software verdeckte Funktionalitäten und unzulässige Zugriffsmöglichkeiten auf von dieser generierte Daten enthält. Auch eine datenschutzrechtliche Prüfung ist ohne Einbeziehung des Quellcodes nicht möglich.

Da dem BKA und dem ZKA die Quellsoftware zu keinem Zeitpunkt vorlag, waren diese Behörden nicht in der Lage, die Funktionalität der von ihnen eingesetzten Programme zu beurteilen. Dies gilt umso mehr, als ihnen noch nicht einmal eine hinreichende Programmdokumentation zur Verfügung stand.

Auch mir ist eine belastbare und abschließende Aussage über die programmierten Funktionen und die Zugriffsmöglichkeiten der eingesetzten Software aus den genannten Gründen nicht möglich.

Das Vorhandensein von nicht zulässigen Funktionen kann damit nicht ausgeschlossen werden. Eventuell vorhandene und genutzte nicht dokumentierte Funktionalitäten können auch nicht vom Betroffenen bemerkt und geahnt werden, weil der Einsatz der Überwachungsmaßnahme insgesamt verdeckt erfolgt. Sie könnte aber auch nicht von der verantwortlichen Behörde nachvollzogen werden, weil deren Existenz dort nicht bekannt ist. Vor diesem Hintergrund ist das Nichtvorhandensein des Quellcodes bei BKA und Zollfahndungsdienst ein schwerwiegender Verstoß gegen die Regelungen des § 9 BDSG nebst Anlage und des § 20k BKAG, dessen Beanstandung ich mir vorbehalte.

In der Gesetzesbegründung zu § 20 k Abs. 3 BKAG wird darauf verwiesen, dass zur Dokumentation zumindest eine Kopie der eingesetzten Software aufzubewahren ist, „damit im Zweifelsfall z.B. ein gerichtlich bestellter Sachverständiger sich davon überzeugen kann", ob die gesetzlichen Anforderungen eingehalten werden.[28] Eine Kopie des Binärcodes ist mir vom BKA nicht übergeben worden. Ungeachtet dessen ist für eine Dokumentation der Quellcode erforderlich, da die Analyse des Binärcodes nicht mit derselben Fehlerfreiheit und Vollständigkeit möglich ist. Beschränkt sich die Analyse auf den Binärcode kann praktisch nicht festgestellt werden, ob eine Programmfunktion nicht vorhanden ist, um etwa auszuschließen, dass eine unberechtigte Funktion implementiert war.

Beim ZKA stellt sich die Situation noch problematischer dar, da dort auch der Binärcode beim ZKA nicht vorgehalten wurde. Zwar soll der Binärcode von DigiTask erneut abgerufen werden können, dies bedeutet jedoch einen deutlichen Zusatzaufwand und aufgrund der Anpassung des Codes für eine Maßnahme eine potentielle Fehlerquelle, die eine sichere Nachvollziehbarkeit weiter erschwert. Die gesetzlich gebotene Dokumentation wird quasi von der Firma DigiTask übernommen. Eine Prüfung, ob und inwieweit diese die Anforderungen erfüllt, hat nicht stattgefunden. Dies stellt insgesamt einen schweren Verstoß gegen gesetzliche Anforderungen dar.

Im Hinblick darauf, dass das BKA auf meine Nachfrage inzwischen mitgeteilt hat, die Firma DigiTask sei bereit, den Quellcode in ihren Geschäftsräumen – vor Ort – zur Einsicht zur Verfügung zu stellen, ist folgendes zu bemerken:

---

[28] BT-Drs. 16/9588, S. 28.

- Die Auswertung des Quellcodes ist mit einem erheblichen zeitlichen und personellen Aufwand verbunden. Darüber hinaus kann es erforderlich sein, dafür technische Hilfsmittel bzw. Tools zu verwenden. Auch sind nach einer ersten Sichtung des Quellcodes ggf. weitere Maßnahmen notwendig, um eine vertiefte Analyse vorzubereiten und durchzuführen. Diese Voraussetzungen sind jedoch bei einer Einsichtnahme vor Ort nicht gegeben.

- Zum anderen ist eine Zuordnung des Quellcodes zu dem Binärcode der tatsächlich in der Praxis eingesetzten Software nicht eindeutig herstellbar. Eine Dokumentation des Zusammenhanges hätte bereits in den Unterlagen des BKA und des ZKA bzw. des jeweiligen ZFA als verantwortlicher Stelle vorgenommen werden müssen. Eine solche Dokumentation hätte beispielsweise dadurch erfolgen können, dass zusammengehörige Kopien von Quell- und Binärcode der jeweils eingesetzten Versionen aufbewahrt worden wären und ggf. Signaturzeichen (Hash-Codes) hinterlegt worden wären.

Ich werde gleichwohl von der angebotenen Möglichkeit zur Einsichtnahme vor Ort Gebrauch machen, behalte mir aber vor, im Hinblick auf die erforderlichen Prüfungsschritte einen weiter gehenden Zugriff auf die Software zu fordern. Das BKA und das ZKA sehe ich in der Pflicht, mir entsprechende Prüfungen zu ermöglichen.

b) Sicherheit der Datenübertragung

Nicht nur die Software, sondern auch die ausgeleiteten Daten müssen sicher vor unberechtigter Kenntnisnahme, Manipulationen und versehentlichen Änderungen geschützt werden. Von zentraler Bedeutung ist dabei die kryptographische Verschlüsselung von Daten, die gleichermaßen deren Vertraulichkeit und Integrität sicherstellen kann.

Die Verschlüsselung der Datenströme ist auch gemäß Ziffer 4 der Anlage zu § 9 BDSG Satz 1 (Weitergabekontrolle) geboten. Gemäß Satz 3 dieser Anlage sind dabei Verfahren einzusetzen die dem Stand der Technik entsprechen. Diese Anforderung ergibt sich zudem auch aus § 20k Abs. 2 BKAG.

Aufgrund der Aussagen des BKA während des Kontrollbesuchs und meiner Feststellungen vor Ort gehe ich davon aus, dass eine Verschlüsselung nach dem Advanced Encryption Standard (AES) eingesetzt wurde. Der dabei verwendete Schlüssel war fest in den Programmcode implementiert. Vor Ort habe ich festgestellt, dass der Pro-

grammcode denselben Schlüssel enthält, den der CCC bei seiner Analyse aus ihm zugänglichen Datenträgern extrahiert hat und der nachfolgend veröffentlicht wurde.

Hierzu hat das BKA allerdings im Nachgang ausgeführt: „Es mag sein, dass der oben genannte Meldetext per Editor lesbar gemacht werden konnte. Allerdings kann im Rahmen Ihrer Prüfung im BKA nicht untersucht und festgestellt worden sein, in welchem Kontext unter welchen technischen Rahmenbedingungen der Text Verwendung findet, und ob die Aussagen des Chaos-Computer-Club (CCC) tatsächlich zutreffen." Statt dieser kryptischen Formulierung hätte ich vom BKA eine Aussage erwartet, ob die von mir geäußerte Annahme zutrifft oder ob ein anderer Schlüssel verwendet wurde. Offenbar ist aber das BKA – mangels detaillierter Kenntnis der von ihm verwendeten Software - selbst zu einer solchen klaren Stellungnahme nicht in der Lage.

Außerdem würde die Aussage des BKA nur dann ein Mindestmaß an Plausibilität besitzen, wenn der Schlüssel zwar nach wie vor im Programmcode enthalten ist, dieser aber gleichzeitig deaktiviert und durch einen weiteren Schlüssel ersetzt worden wäre. Eine solche Programmiertechnik würde angesichts der Eingriffsintensität der Maßnahme zumindest Fragen aufwerfen, etwa danach, ob neben den offiziellen noch weitere verdeckte Zugriffsmöglichkeiten bestehen.

Hieran zeigt sich nochmals, dass hohe Anforderungen an die Dokumentation des technischen Verfahrens zu stellen sind; insbesondere ohne einen Rückhalt des Quellcodes lässt sich ansonsten auch die Qualität einer in den Programmcode integrierten Verschlüsselung nicht mehr beurteilen.

Dem Stand der Technik entsprechen Sicherungsmaßnahmen dann, wenn das nach dem jeweiligen Entwicklungsstand technisch-praktisch realisierbare umgesetzt wurde).[29] Es existieren in die technische Praxis eingeführte effektivere Verfahren, die benutzt werden können, um die Daten hinreichend zu schützen.

Bei dem in der Software verwendeten Verschlüsselungsstandard AES handelt es sich um ein symmetrisches Verfahren, das im Oktober 2000 als Standard bekannt gegeben wurde. Symmetrische Verfahren haben die Eigenschaft, dass zum Ver- und Entschlüsseln derselbe Schlüssel verwendet wird. Dieser Schlüssel ist deshalb geheim zu halten. Der Zugang zum Schlüssel ermöglicht die Entschlüsselung von Daten.

---

[29] Schulte, Beck'scher Kommentar Umweltrecht, § 3 BImSchG, Rn. 92; vgl. Simitis, Bundesdatenschutzgesetz, 7. Auflage 2011, § 9 Rn. 171.

Die Implementierung des Verfahrens sieht die Speicherung des geheimen Schlüssels im ausführbaren Programm (Binärcode) der DigiTask Software vor. Der Schlüssel wird von der Firma DigiTask einprogrammiert und ist zudem nur durch Mitarbeiter dieser Firma änderbar. Der Kreis der Personen die Kenntnis über den Schlüssel haben, erstreckt sich somit auf:

1. Aktuelle und ehemalige Mitarbeiter des BKA in der IT-Administration die Zugang zur ausführbaren Software haben bzw. hatten,
2. aktuelle und ehemalige Mitarbeiter anderer Bedarfsträger, die ebenfalls diese DigiTask-Software einsetzten,
3. aktuelle und ehemalige Mitarbeiter der Firma DigiTask, die die Software programmiert haben und/oder die Zugang zur Software zu Testzwecken benötigen,
4. alle übrigen Personen, die Zugang zur Software haben und über entsprechende IT-Kenntnisse verfügen (beispielsweise der Betroffene selbst).

Der Schutz des verwendeten Schlüssels ist damit nicht steuerbar. Auch unbefugte Dritte mit Zugriff auf den Binärcode, die über entsprechende IT-Kenntnisse verfügen, können den Schlüssel, der unbedingt geheim zu halten wäre, zur Kenntnis nehmen. Die Verwendung eines symmetrischen Verfahrens zur Verschlüsselung ist – jedenfalls bei fest einprogrammiertem Schlüssel - mit unvertretbaren Sicherheitsrisiken verbunden.

Wie bereits oben erwähnt, ist die Änderung des Schlüssels nicht vorgesehen. Dies hat zur Folge, dass verschiedene Überwachungsmaßnahmen, bei denen die DigiTask Software eingesetzt wurde, mit dem gleichen Schlüssel verschlüsselt und gesichert wurde. Mitarbeiter der Firma DigiTask oder andere Nutzer der DigiTask-Software hätten somit die Möglichkeit die Schlüssel einzusetzen, um Daten zu entschlüsseln oder (evtl. veränderte) Daten zu verschlüsseln. Die Vertraulichkeit ist damit nicht hinreichend sichergestellt.

Weitere Faktoren für die Sicherheit ist die konkrete Implementierungen des Algorithmus und die Zuverlässigkeit der verwendeten Hintergrundsysteme. Beides konnte ich nicht prüfen, weil mir keine Analyse des Quellcode möglich war. Die Ausführungen im CCC-Report geben Anlass zur Nachfrage, ob der Algorithmus korrekt umgesetzt wurde.

Bei den Hintergrundsystemen ist der Proxy-Server einerseits in seinem Funktionsumfang relativ überschaubar, andererseits durch den Standort in einem externen Rechenzentrum schwerer kontrollierbar. Sowohl die Verschlüsselung mit einem einheitlichen Schlüssel und das offensichtlich nicht optimal umgesetzte Verschlüsselungs-

verfahren, als auch die Protokollierung waren mit vermeidbaren Risiken verbunden,. Durch die nicht vorhandene Dokumentation wird diese Schwachstelle noch verstärkt.

Da beim ZKA keine Kopie der Überwachungssoftware vorhanden war, konnte keine separate Prüfung durchgeführt werden, etwa um zu bestätigen, dass es sich um den gleichen Schlüssel handelt.

Die Sicherheit der Verschlüsselung ist abhängig von dem eingesetzten Verschlüsselungsverfahren, der Schlüssellänge und der Implementierung des Verfahrens.
Die Übertragung von bei der Quellen-TKÜ ausgeleiteten Daten unter Verwendung eines Verschlüsselungsverfahrens mit in die Überwachungssoftware fest einprogrammiertem Schlüssel durch das BKA war nach den genannten rechtlichen Maßstäben ungenügend. Sie entspricht auch nicht dem Stand der Technik. Die Sicherheit der Datenübertragung bei den durch das ZKA durchgeführten Maßnahmen war nicht prüfbar.

Insofern haben beide Behörden gegen § 9 BDSG verstoßen.

c) Authentisierung

Die IT-Sicherheit hängt zum großen Teil davon ab, dass alle am Verarbeitungsprozess beteiligten Daten und Systemkomponenten nur im Rahmen ihrer Zugriffsrechte handeln und dass die Daten nicht unberechtigt verändert oder unterdrückt werden. Dies wiederum setzt eine sichere Feststellung hinsichtlich der Identität aller an den Prozessen Beteiligten voraus. Die dabei eingesetzten Techniken und Verfahren werden als Authentisierung bezeichnet.

Dabei muss zwischen Datenauthentisierung und Instanzauthentisierung unterschieden werden.

Unter Datenauthentisierung werden (kryptographische) Verfahren verstanden, die garantieren, dass übersandte oder gespeicherte Daten nicht verändert wurden und/oder verändert werden können (Anforderung aus § 20 k Ab2. 2 Satz 2 BKAG). Dabei benutzt ein Sender (in diesem Fall die Überwachungssoftware) ein (kryptographisches) Verfahren zur Erzeugung einer Prüfsumme der zu authentisierenden Daten. Der Empfänger prüft dann ob die empfangene Prüfsumme mit der von ihm selbst errechneten Prüfsumme übereinstimmt. Somit kann hinreichend sicher die Unverfälschtheit der empfangenen Daten und die Richtigkeit des Senders festgestellt werden. Die Prüfsumme bleibt während der gesamten Speicherdauer erhalten. Der

Schutz erstreckt sich somit nicht nur auf die Übertragung, sondern auch auf die Speicherung der Daten.

Unter Instanzauthentisierung werden (kryptographische) Protokolle verstanden, in denen ein Empfänger (z. B. BKA) einem Sender (Überwachungssoftware) den Besitz eines Geheimnisses nachweist. Bei symmetrischen Verfahren ist dies ein symmetrischer Schlüssel. Sowohl die Daten- als auch die Instanzauthentisierung erfolgt meist gegenseitig und geht mit einer Schlüsseleinigung einher, um die Vertraulichkeit und Integrität zu gewährleisten. Die Verfahren müssen den Anforderungen der Technischen Richtlinie 02102 des BSI (Kryptographische Verfahren: Empfehlungen und Schlüssellängen) angepasst werden. Das BSI empfiehlt darin die Anwendung unterschiedlicher Verfahren zu Sicherstellung der Authentizität. Im Falle des Einsatzes der Überwachungssoftware muss aus folgenden Gründen auf die Sicherheit der Verfahren geachtet werden:

- Sicherstellung der Unversehrtheit und Unverfälschtheit der Daten,
- Richtigkeit des Senders (Nichtabstreitbarkeit des Senders),
- Richtigkeit des Empfängers (Nichtabstreitbarkeit des Empfängers),
- Richtigkeit des Senders im Falle der Steuerung der Software (also aus der Sicht des BKA muss sichergestellt sein, dass Steuerungseingriffe (Nachladefunktion) auch nur vom BKA ausgeführt wurden.

Bei der vorliegenden Software wurde das zur Verschlüsselung verwendete AES-Verfahren auch zur Daten- und Instanzauthentisierung mit fest programmierten Schlüssel eingesetzt.

Der Einsatz eines symmetrischen Verfahrens sowohl für die Daten- als auch für die Instanzauthentisierung ist aus den oben erwähnten Gründen unzureichend. Es wird nur der Übermittlungsweg selbst abgesichert (und dies auch nur, soweit ein möglicher Angreifer den verwendeten Schlüssel nicht kennt), die Unverfälschtheit der Daten während der Speicherung und gar die Richtigkeit des Senders bzw. Empfängers eben nicht. Das hat zur Folge, dass nicht ausgeschlossen werden kann, dass Dritte die Rolle „BKA" oder „Zielrechner" übernehmen, ohne dass diese „Übernahme" durch BKA oder das Zielsystem erkannt wird. Der Einsatz des Verschlüsselungsverfahrens zur Datenauthentisierung entspricht deshalb nicht dem Stand der Technik und ist deshalb nicht ausreichend.

Die Ergänzung der Instanzauthentisierung im BKA durch Eingabe einer Benutzerkennung und eines Passwortes zur Verwaltung der Daten und zur Steuerung der Überwachungssoftware reicht nicht aus. Die Sicherheit des eingesetzten Verfahrens

wird gemäß dem eGovernment Handbuch des BSI (Kapitel „Merkmale von Authentisierungs-Mechanismen") nur mit der kleinsten Stufe „niedrig" bewertet. Eine hinreichende Instanzauthentisierung wird dadurch nicht erreicht. Höherwertige Verfahren basieren auf Chipkartenverfahren. Auf solche Verfahren wurde aber beim Einsatz der Überwachungssoftware verzichtet.

Die in der vom BKA Überwachungssoftware verwendete Authentisierung ist als schwach zu bezeichnen. Sie erfüllt nicht die Anforderungen aus Ziffer 3 (Zugriffsschutz) der Anlage zu § 9 BDSG sowie den Anforderungen aus § 20k Abs. 2 BKAG und stellt damit einen erheblichen Mangel dar.

d) Benutzerverwaltung in der Recording-Unit (RU)

Aus Gründen der Instanzauthentisierung muss sich jeder Nutzer authentisieren, der die Überwachungssoftware bedient oder der Daten mittels der Überwachungssoftware verarbeitet oder nutzt. Diese Authentisierung muss sicherstellen, dass nachvollzogen werden kann, welcher Nutzer, wann welche Daten verarbeitet und/oder genutzt hat. Daraus folgt, dass nur Benutzerkennungen verwendet werden können, die sich eindeutig auf eine Person beziehen. Gruppenkennungen, hinter denen sich mehrere Personen verbergen, sind dazu nicht geeignet, weil die Nachvollziehbarkeit der Verarbeitung und/oder Nutzung der Daten nicht lückenlos gewährleistet werden kann.

Vor diesem Hintergrund stellt die Gruppenkennung „Übersetzer" auf dem RU des BKA einen Verstoß gegen Vorschriften der Ziffer 3 der Anlage zu § 9 BDSG dar. Die Gruppenkennung ermöglicht es nicht nachzuvollziehen wer die personenbezogenen Daten zu welcher Zeit verarbeitet hat. Die Einrichtung einer individuellen Kennung ist angesichts der Schutzwürdigkeit der Daten angezeigt, insbesondere unter den Aspekten der besonderen Bedrohungen.

e) Protokollierung und Löschung der Protokolle

§ 20l Abs. 2 Satz 2 i. V. m. § 20k Abs. 3 BKAG fordert eine Protokollierung u. a. der Angaben, die die Feststellung der erhobenen Daten ermöglicht. Diese Protokolldaten dürfen nur für Prüfungen, etwa bei der gerichtlichen oder der Datenschutzkontrolle, verwendet werden.

Die vorhandenen Protokolle in Verbindung mit anderen Informationen ermöglichen zwar eine gute Nachvollziehbarkeit der Aktionen/Zugriffe, entsprechen aber sonst –

z.B. hinsichtlich der Form – nicht den gesetzlichen Regelungen, die implizit eine separate Speicherung und Löschung der Protokolldaten voraussetzen.[30] Beispielsweise wäre eine Auskunft an den Betroffenen nur der in § 20k Abs. 3 Satz 1 BKAG genannten Daten nicht ohne umfangreiche manuelle Aufbereitung möglich. Diese wäre fehleranfällig und könnte theoretisch leicht manipuliert werden. Auch im Sinne von Ziffer 8 der Anlage zu § 9 BDSG wäre eine Trennung der Protokolle zur Datenschutzkontrolle und der für die Strafverfolgung genutzten Daten angezeigt.

In den Protokollen sind nicht die erhobenen Daten selbst zu speichern.[31] Weiter ist eine automatisierte Löschung der Protokolle vorzusehen. Eine solche findet nicht statt. Die gesetzliche Vorgabe wird insofern nicht eingehalten.

Zu den einzelnen in § 20k Abs. 3 Satz 1 BKAG geforderten Gegenständen der Protokollierung kann folgendes gesagt werden:

aa) Bezeichnung des technischen Mittels und der Zeitpunkt seines Einsatzes

In der RU wird der Hash-Wert der Quellen-TKÜ-Software protokolliert. Ferner wurde beim BKA die Software im Lieferzustand und mit IP-Adresse und U-Nummer versehen gespeichert. Bei der Lieferung hat die Firma DigiTask auch die jeweiligen Versionsnummern und Fähigkeiten der Software in einer Textdatei beigefügt. Somit war beim BKA zumindest prinzipiell nachvollziehbar, welches technische Mittel verwendet wurde, auch wenn die Prüfbarkeit der eingesetzten Software mangels Dokumentation und Quellcodekenntnis unzureichend war. Dagegen hatte das ZKA die Software nicht gespeichert. Somit ist dort eine Nachvollziehbarkeit nicht erfüllt.

Der Einsatzzeitpunkt (im Sinne von erster Kontaktaufnahme mit der RU) war beim BKA und beim ZKA anhand der Protokollierung in der RU nachvollziehbar, sobald die Software sich dort anmeldete. Die Aufbringung selbst – etwa ein Aufspielen – war technisch nicht protokolliert könnte allenfalls anhand anderer Informationen nachvollzogen werden.

bb) Angaben zur Identifizierung des informationstechnischen Systems und zu den daran vorgenommenen nicht nur flüchtigen Veränderungen

[30] Siehe auch BT-Drucksache 16/9588, Begründung zu § 20k Abs. 3 Satz 2 , S. 28 links unten.
[31] Siehe BT-Drucksache 16/9588, Begründung zu § 20k Abs. 3 Satz 1 Nr. 3, S. 28 links

Welches informationstechnische System mittels Quellen-TKÜ überwacht wurde, also ob der richtige Rechner „infiziert" wurde, war anhand der von der RU protokollierten Daten nur durch Heranziehung der Software-Liste und der IP-Adresse annähernd nachvollziehbar. Dabei handelt es sich jedoch nicht um eindeutige Angaben. Eine eindeutige Identifizierung des Zielrechners könnte bei der Einbringung der Software durchgeführt worden sein oder kann sich anhand anderer Informationen ergeben (z. B. wenn IP-Adresse von einer parallel durchgeführten TKÜ-Maßnahme bekannt ist und es sich um den einzigen Rechner im Haushalt handelt). Diese Informationen sind aber ggf. an anderer Stelle niedergelegt, z. B. der Fallakte. Wie sicher ein System identifiziert werden kann, ist in jedem Einzelfall unterschiedlich.

Bei den „nicht nur flüchtigen Veränderungen" handelt es sich zumindest um das Aufbringen von zwei Dateien. Dies wird nicht explizit protokolliert, das BKA verfügt jedoch über diese Information. Ob weitere Änderungen durchgeführt werden, z. B. eine Änderung an der Registry, ist nicht bekannt. Hier wäre eine detaillierte Beschreibung der Funktionsweise der Software oder Untersuchung des Quellcodes erforderlich, der leider nicht vorliegt.

cc) Angaben, die die Feststellung der erhobenen Daten ermöglichen

Es werden alle erhobenen Daten in der RU gespeichert. Damit kann anhand der Protokolle nicht nur nachvollzogen werden, wann welche Daten erhoben wurden (Metadaten), sondern auch die vollständigen Inhalte. Eine getrennte Protokollierung, die nur eine Feststellung der erhobenen Daten ermöglicht, ohne dass die Daten selbst (also etwa die Gesprächsinhalte oder der Texte eines Chats) enthalten wären, findet nicht statt.

dd) Organisationseinheit, die die Maßnahme durchführt

Eine explizite Protokollierung zu diesem Punkt war nicht zu erkennen. Die beteiligten Organisationseinheiten ergaben sich insoweit aus der Aktenlage.

Die Betrachtung der einzelnen Forderungen zeigt auf, dass die geforderten Informationen weitgehend vorhanden sind, aber nicht in Form der geforderten Protokollierung.

Durch die Mehrfachspeicherung (vgl. B VI 2. b)) wird im ZKA zusätzlich zur Protokollierung der Maßnahme in der Recording-Unit auch im vorhandenen System für die klassische TKÜ eine Protokollierung durchgeführt. Eine Protokollierung in genau der Form, wie sie im BKA-Gesetz gefordert wird, findet ebenfalls nicht statt. Es wäre allerdings zu diskutieren, ob die im BKA-Gesetz geforderte Form auch vom ZKA verlangt werden konnte.

f) Die Nachladefunktion

Prinzipiell bietet die Nachladefunktion die Möglichkeit, auf einem Zielsystem zusätzliche Software zu installieren oder vorhandene Software zu verändern oder zu deinstallieren. Wegen ihrer besonderen Flexibilität stellt sie einen besonders kritischen Faktor der eingesetzten Überwachungssoftware dar, vor allem im Hinblick auf die gesetzlich und verfassungsrechtlich gebotene Beschränkung der Überwachung auf die laufende Telekommunikation.

Ob schon das Aufbringen einer Funktion zum Nachladen von Software einen Verstoß gegen diese gesetzlichen Vorgaben darstellt, oder erst deren unzulässige Aktivierung und Nutzung, ist schwierig zu beantworten. Eine entsprechende Bewertung setzt die abschließende Kenntnis der Funktionalitäten der Überwachungssoftware und der gegen Missbrauch der Nachladefunktion getroffenen Schutzmaßnahmen voraus – Voraussetzungen, die auf Grund der fehlenden Dokumentation und Quellcodeanalyse nicht gegeben sind.

Das BKA hält die die Nachladefunktion für erforderlich, um die Überwachungssoftware an die normalen Updates auf dem Zielcomputer anpassen zu können. Allerdings wird diese Funktion vom BKA auch verwendet, um die Überwachungssoftware mit aktiver Überwachungsfunktion bei Beginn der Maßnahme auf dem Zielsystem zu installieren.

Das Nachladen unzulässiger Funktionen könnte durch eine starke Instanzauthentisierung verhindert werden, die hier allerdings – wie oben ausgeführt – nicht vorliegt. Darüber hinaus zwingen die mit der Nachladefunktion verbundenen Risiken zu einer revisionssicheren automatisierten Protokollierung. Kontrollierbar ist sie zudem nur dann, wenn der Programmcode zur Verfügung steht und eventuell zur Prüfung offengelegt ist.

Bei meinem Kontrollbesuch habe ich keine Anhaltspunkte festgestellt, dass das BKA gezielt unzulässigen Funktionen nachgeladen oder aktiviert hat.

Vom ZKA wurde – anders als vom BKA – die Nachladefunktion nicht verwendet. Ein Verzicht auf die Nachladefunktion hat einerseits den Vorteil, dass die hier angesprochene Problematik nicht mehr relevant ist. Andererseits müsste ohne Nachladefunktion die Software ggf. mehrfach neu aufgebracht werden. Falls die Software auf einem falschen Rechner installiert würde, wäre dieser mit einer funktionsfähigen Quellen-TKÜ-Software versehen, ohne dass dieses Versehen rückgängig gemacht werden könnte.

Im Hinblick auf diese Problemlage bedürfen die Nachladefunktion selbst und die Anforderungen an ihre Ausgestaltung weiterer Analyse.

g) Reichweite und Löschung der Überwachungssoftware

Die Quellen-TKÜ-Software soll ein informationstechnischen System nur soweit verändern, wie dies für die Überwachungsmaßnahme erforderlich ist.

Inwieweit das Aufbringen von Software erforderlich ist und welche Funktionen sie aufzuweisen hat, hängt eng mit den zu überwachenden Zielsystemen und den von den Beschuldigten verwendeten Kommunikationsprogrammen zusammen. Soll z.B. die Kommunikation über Skype überwacht werden, dürfen darüber hinaus in der Software keine weiteren Funktionalitäten vorhanden sein.

Ohne Analyse des Quellcodes ist mir eine abschließende Bewertung, welche Funktionen in der auf Zielsystemen aufgebrachten Software implementiert waren, derzeit nicht möglich. Die von mir gesichteten Protokolle und sonstigen Unterlagen über durchgeführte Überwachungsmaßnahmen haben keine Anhaltspunkte dafür ergeben, dass vom BKA und ZKA Funktionen genutzt wurden, die über die gesetzlichen Anforderungen hinausgehen. Leider stand zur meiner Prüfung weder der Quellcode zur Verfügung, noch wurde mir der vorhandene Binärcode zur Analyse übergeben.

Nach Abschluss der Maßnahme soll die Löschung der Überwachungssoftware über einen Steuerbefehl (Remote) erfolgen. Die Löschung setzt also zumindest einen fortgesetzten Online-Zugriff des BKA auf das Zielsystem voraus. Sollte dieser Zugriff auf Grund zusätzlicher Sicherungsmaßnahmen des Betroffenen (etwa durch Einsatz verbesserter Virenschutzsoftware) nicht mehr möglich sein, bliebe das Überwachungsprogramm weiterhin aktiv.

Der ausgelöste Löschvorgang ist allerdings dann nur ein logisches Löschen. Die Software kann deshalb mit geringem Aufwand wieder hergestellt werden, und zwar nicht nur durch den Bedarfsträger sondern ggf. auch durch andere Personen, die Zugang zu dem System haben. Auf den Einsatz eines Programms zum „physikalischen Löschens" durch Überschreiben hat das BKA verzichtet. Es hat allerdings mitgeteilt, dass im Falle einer Beschlagnahme des Rechners die Löschung noch vorhandener Daten vor Ort erfolge.

Festzuhalten bleibt allerdings, dass bei einer Beschlagnahme des Rechners die eingebrachte Software durch physikalisches Überschreiben gelöscht werden kann. Die Anforderungen aus § 20 k BKAG wären erst dann umgesetzt. Der Deaktivierungsmechanismus bedarf auch im übrigen weiterer Analyse, die ohne entsprechende Quellcodekenntnis nicht möglich ist.

h) Alternative Zugriffsmöglichkeiten

Laut Presseberichten haben andere Staaten (beispielsweise Italien) mit Unternehmen wie Skype Möglichkeiten zur Entschlüsselung von VoIP-Telefongesprächen vereinbart. Auch wären die Möglichkeiten, die verschlüsselten Datenströme bei VoIP-Gesprächen ohne Unterstützung der Softwarehersteller (Skype usw.) zu entschlüsseln, zu untersuchen und zu bewerten.

Ein direktes Entschlüsseln der Daten beim „Provider oder mit dessen Hilfe" wäre – wie die konventionelle TKÜ – ein deutlich geringerer Eingriff als die Quellen-TKÜ. Mir ist nicht ersichtlich, warum die deutschen Bedarfsträger nicht diesen Weg gegangen sind.

3. Begrenzung auf bestimmte Telekommunikationsanschlüsse

Die Reichweite der zulässigen Maßnahme ergibt sich aus dem jeweiligen gerichtlichen Beschluss. Wesentlicher Bestandteil der Entscheidungsformel der gerichtlichen Beschlüsse in strafprozessualen Fällen gemäß § 100b Abs. 2 Satz 2 Nr. 2 StPO „die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Gerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist". Damit wird konkret festgelegt, welche Geräte und welche Telekommunikationsverbindungen überwacht werden dürfen und welche Telekommunikationsanbieter zur Mitwirkung verpflichtet sind.

Wie genau die Gerichte diese Festlegungen treffen müssen, habe ich nicht zu bewerten. Soweit die Ausführung der datenschutzrechtlichen Kontrolle unterliegt, betrifft diese allerdings auch die Frage, ob sich die kontrollierten Sicherheitsbehörden innerhalb der von den Gerichten vorgegebenen Tenorierung bewegt haben.

Technisch gesehen findet die Quellen-TKÜ unabhängig vom Provider oder bestimmten Anschlüssen statt. Die Überwachungssoftware wird auf dem – in einigen Beschlüssen jeweils ausdrücklich benannten – Zielgerät aufgebracht und aktiviert. Sobald die Überwachungssoftware „bemerkt", dass das Zielgerät online ist, leitet sie die Telekommunikation auf dem oben beschriebenen Weg an die Polizeibehörde aus. Dabei arbeitet die Software völlig unabhängig davon, ob der Nutzer des Geräts dieses an einen bestimmten Telekommunikationsanschluss angeschlossen hat. Die Software arbeitet zum Beispiel auch dann, wenn der Nutzer über den WLAN-Anschluss eines Nachbarn, eines Freundes, eines Hotels oder über einen Hotspot online geht. Die Software unterscheidet zudem nicht danach, ob dieser weitere Anschluss im In- oder Ausland liegt.

Die vorliegenden gerichtlichen Beschlüsse waren insofern recht unterschiedlich tenoriert. Teilweise enthielten die gerichtlichen Beschlüsse keine Begrenzung auf einen bestimmten Telekommunikationsanschluss. Insoweit konnte auch keine durch das Gericht gesetzte Beschränkung überschritten werden.

Anders liegt dies jedoch in den Fällen, in denen sich die gerichtliche Anordnung auf einen bestimmten Telekommunikationsanschluss bezog (z.B. „Überwachung und Aufzeichnung sämtliche über die informationstechnischen Systeme des Beschuldigten [...] kryptisiert geführte Telekommunikation zum Anschluss [...] (DSL-Leitung)".

Strukturell war durch die eingesetzte Software jedoch – wie ausgeführt – nicht sichergestellt, dass nur über diesen Anschluss ausgeleitete Verbindungen überwacht werden. Wie oben ausgeführt, leitet die auf dem Computer des Beschuldigten installierte Überwachungssoftware Inhalte zur Überwachungseinheit der ermittelnden Behörde unabhängig von den genutzten Telekommunikationsanschlüssen aus. Die Software enthielt auch keine Funktion, die eine Ausleitung abschaltete, wenn von einem anderen als dem im gerichtlichen Beschluss genannten Anschluss kommuniziert wurde.

Ich habe nicht in allen Einzelfällen der Frage nachgehen können, ob der Rechner der jeweiligen Beschuldigten auch an anderen, nicht im jeweiligen Beschluss genannten Anschlüssen verwendet worden ist. Dass dies vorgekommen ist, zeigt die oben unter B. I. 7. und B. II. 7. aufgeführten Fallkonstellation, in der die überwachte Personen

die Spähsoftware erst im Ausland und somit über einen anderen als den im Gerichtsbeschluss genannten Anschluss auf dem eigenen Laptop verwendete. Damit wird deutlich, dass es sich – bezogen auf die Umsetzung der richterlich festgelegten Eingrenzungen – um einen strukturellen Mangel der Vorgehensweise handelt, der auch zumindest in einem Fall konkret relevant wurde.

Damit ist festzustellen, dass die Vorgaben der gerichtlichen Beschlüsse insoweit teilweise überschritten wurden. Ob es sich dabei um eine nach §§ 20k, 20l BKAG bzw. § 100a StPO ggf. in Verbindung mit dem Grundsatz der Verhältnismäßigkeit zu beachtende allgemeine Anforderung oder um spezielle Berücksichtigungen besonderer Einzelfälle handelt, habe ich nicht zu bewerten. Entscheidend ist im vorliegenden Zusammenhang, dass die Beschränkung auf bestimmte Telekommunikationsanschlüsse durch die gerichtlichen Beschlüsse angeordnet war, die auch für meine datenschutzrechtliche Kontrolle insoweit bindend sind. Dagegen wurde insofern verstoßen.

4. Räumliche Reichweite

Aus den vorstehenden Ausführungen ergibt sich auch, dass die auf dem Zielsystem angesetzte Überwachungssoftware nicht danach unterscheidet, ob die Kommunikation aus dem Inland erfolgt, oder über einen ausländischen Telekommunikationsanschluss. Das ist insbesondere in Fällen relevant, in denen der oder die Beschuldigte ein mobiles Gerät mit ins Ausland nimmt.

Wie oben beschrieben, ist es in einem Verfahren nach Darstellung des BKA dazu gekommen, dass vom europäischen Ausland aus Gespräche des Beschuldigten ausgeleitet wurden. Bei den Telekommunikationsüberwachungen der ZFÄ ist diese Konstellation mindestens zweimal aufgetreten (siehe unter B.II.7.)).

In solchen Fällen ist innerhalb der EU Art. 20 des Europäischen Rechtshilfeübereinkommens (EU-RhÜbk) zu beachten. Dieser regelt eine passive Form der Amtshilfe bei einer mobilen Zielperson in Fällen, in denen diese sich in das Hoheitsgebiet eines anderen Mitgliedsstaats begibt und den überwachten Anschluss – bzw. hier das überwachte Endgerät – von dort aus nutzt.[32] Hatte das BKA Kenntnis, bevor der Beschuldigte in das Ausland ging, wäre der betroffene Staat gemäß Art. 20 Abs. 2 Buchst. a i.V.m. Abs. 3 EU-RhÜbk. vor der Überwachung zu unterrichten. In anderen Fällen hätte diese Pflicht nach Kenntniserlangung bestanden, Art. 20 Abs. 2 Buchst. b EU-RhÜbk. Für den Bereich außerhalb der EU gelten die allgemeinen Rechtshilfe-

[32] vgl. Schuster NStZ 2006, 657, 660.

regeln. Wenn technisch gesehen auf ein Gerät Zugriff genommen wird, welches sich zum Zugriffszeitpunkt im Ausland befindet, handelt es sich um einen in das Hoheitsgebiet des ausländischen Staats ausgreifenden hoheitlichen Akt; dies ist grundsätzlich nur im Wege eines Rechtshilfeersuchens möglich.[33] Soweit eine vorläufige Sicherung für grundsätzlich zulässig angesehen wird,[34] ist das Rechtshilfeersuchen nicht erst zu stellen, wenn es um die Verwertbarkeit der Beweise geht. Denn der Grundrechtseingriff erfolgt nicht erst mit der Verwertung der Beweise, sondern bereits bei der Erhebung und bedarf daher einer vorherigen Rechtfertigung. Darüber hinaus spricht vieles dafür, dass auch die vorläufige Sicherung einer ausdrücklichen Regelung bedarf, wie dies etwa bei § 20 Abs. 2 des EU-RhÜbk. der Fall ist, der dazu allerdings eine ausdrückliche Unterrichtungspflicht enthält.

Vorliegend sind die Darstellungen des BKA widersprüchlich. Im Gespräch während des Kontrolltermins wurde uns mitgeteilt, dass im betreffenden Fall Erkenntnisse aus Begleitmaßnahmen vorgelegen hätten, nach denen der Beschuldigte „Skype" auch vom Ausland aus genutzt habe. Im Schreiben vom 20.12.2011 führte BKA dann allerdings aus, dass hinsichtlich der Unsicherheit bei möglichen Auslandsaufenthalten im konkreten Verfahren der Staatsanwaltschaft die eingeschränkten technischen Gegebenheiten dargestellt worden seien. Diese habe daraufhin entschieden, dass die Maßnahme aufgrund der technischen Unsicherheiten im vollen Umfang weiterzuführen sei. Insofern ist nicht nachvollziehbar, dass auf der einen Seite mit den technischen Unsicherheiten argumentiert wird, auf der anderen Seite aber aufgrund von Begleitmaßnahmen der Aufenthaltsort des Beschuldigten zumindest annäherungsweise bestimmbar war.

Dazu ist im vorliegenden Fall zu ergänzen, dass es sich um ein Ermittlungsverfahren im Bereich der organisierten Kriminalität handelte. In solchen Fällen ist es üblich – und wurde nach Darstellung des BKA auch hier praktiziert – die „gesamte Klaviatur" strafprozessualer Maßnahmen auszuschöpfen (aus Gründen der Verhältnismäßigkeit ist es ohnehin erforderlich, zunächst die weniger eingriffsintensiven Mittel auszuschöpfen, weshalb die Ermittlungen sich ohnehin nie auf die Quellen-TKÜ beschränken dürften). Gleichzeitig ging es inhaltlich um den Verdacht, dass der Beschuldigte aus Südamerika Drogen in die Bundesrepublik einführen wollte, weshalb der Aufenthaltsort für das konkrete Verfahren eine besondere Rolle gespielt hat. Die beschriebene „Unsicherheit" erscheint insoweit nicht nachvollziehbar.

---

[33] vgl. Rau WM 2006, 1281, 1287 m.w.N.; Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 374 ff.
[34] vgl. Bär a.a.O. Rn. 376.

Zu den technischen Unsicherheiten ist zu ergänzen: Im Gegensatz zur Auffassung des BKA dürften Geo-IP-Datenbanken bei regulär genutzten Internetzugängen für Privatkunden (z. B. DSL, Mobilfunk) eine relativ hohe Zuverlässigkeit haben, soweit nicht die Stadt, sondern das Land ermittelt werden soll. Lediglich bei Nutzung von Firmennetzen, bei VPN oder Anonymisierungsdiensten (z. B. TOR) dürfte eine relevante Unsicherheit bestehen, in welchem Land sich ein Nutzer aufhält. Vor diesem Hintergrund bedarf der Sachverhalt weiterer Klärung.

Beim ZKA besteht grundsätzlich eine vergleichbare Problematik. Allerdings können die Ermittler an den Auswerteplätzen die IP-Adresse nicht erkennen. Eine Prüfung, von welcher IP-Adresse Daten übermittelt wurde, erfordert einen erhöhten Aufwand. Insofern dürfte die IP-Adresse – und somit der Standort des überwachten Rechners – im Regelfall nicht beachtet werden. In dem Fall, in dem der Betroffene seinen Computer mit installierter Überwachungssoftware im Ausland verwendete, wurde ausweislich eines Aktenvermerks um Rechtshilfe der estnischen Behörden ersucht. In dem Fall, in dem die Spähsoftware auf dem sich im Ausland befindlichen Computer der Freundin des Beschuldigten installiert wurde, sei die Software unmittelbar wieder deinstalliert und die aufgezeichneten Gespräche gelöscht worden.

5. Amtshilfe

Die vorgefundenen Amtshilfekonstellationen betreffen die Bundespolizei als ersuchende Behörde und das BKA als ersuchte Behörde.

Soweit das BKA in Amtshilfe gehandelt hat, ist für die damit verbundene Erhebung und Verwendung personenbezogener Daten eine eigenständige Rechtsgrundlage erforderlich.[35]

Materiell können sich alle die Maßnahmen durchführenden Behörden zur Erhebung personenbezogener Daten mittels Quellen-TKÜ für die strafprozessuale Telekommunikationsüberwachung allenfalls auf § 100a StPO und die jeweils ergangenen Gerichtsbeschlüsse stützen; insoweit gilt das oben zu I.2.) Gesagte, auch im Hinblick darauf, dass eine Bewertung durch mich im Hinblick auf die richterliche Unabhängigkeit nicht erfolgen kann. Die Amtshilfe ist jedenfalls insofern auch nicht generell unzulässig, weil keine der beteiligten Behörde ihre Eingriffsbefugnisse durch eine Amtshilfemaßnahme erweitert hat.

[35] vgl. BVerfGE 65, 1, 46.

Für die Zulässigkeit der Amtshilfe ist darüber hinaus zu prüfen, ob die beteiligten Behörden Amtshilfe ersuchen bzw. leisten durften und welchen rechtlichen Grenzen sie dabei unterlagen, insbesondere im Hinblick auf die Intensität des Grundrechtseingriffs durch eine Quellen-TKÜ. Die Zulässigkeit dürfte letztlich auch im Falle der Bundespolizei als ersuchender Behörde anzunehmen sein, weil die rechtmäßige Durchführung einer Quellen-TKÜ hohe technische Anforderungen hat, eine große sachliche Nähe zwischen den beteiligten Polizeibehörden besteht und zudem Übermittlungsvorschriften in den jeweiligen Polizeigesetzen vorgesehen sind (vgl. § 32 Abs. 1 BPolG).

Kritisch sehe ich jedoch, dass die Bundespolizei in ihrem Ersuchen an das BLKA auf die besonderen rechtlichen und technischen Anforderungen, die an eine Quellen-TKÜ zu richten sind, nicht gesondert hingewiesen, sondern die technische Umsetzung ohne weitere Ausführungen zu den Besonderheiten des Ersuchens in den Hände des BLKA gelegt hat.

Für das BKA als in verschiedenen Fällen ersuchte Behörde ist die Zuständigkeit für die Durchführung der Maßnahme anzunehmen. Gemäß § 4 Abs. 2 Satz 1 Nr. 1 BKAG ist das BKA zuständig, die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahrzunehmen, wenn eine zuständige Landesbehörde darum ersucht. In seinem Wortlaut „die polizeilichen Aufgaben" betrifft § 4 Abs. 2 Satz 1 Nr. 1 BKAG die Übernahme der gesamten Zuständigkeit, die polizeilichen Aufgaben in einem Ermittlungsverfahren wahrzunehmen. § 17 BKAG sieht als Unterstützungshandlung für Zwecke der Strafverfolgung lediglich die Entsendung von Bediensteten vor.

Gleichwohl wird in der Literatur für zulässig gehalten, ein an das BKA gerichtetes Ersuchen als „Minus" nicht auf die Übernahme des gesamten Ermittlungsverfahrens zu richten, sondern dieses auf einzelne Ermittlungshandlungen zu beziehen.[36] Hierfür spricht nach dem Sinn und Zweck der Vorschrift, dass das BKAG, der Kompetenzverteilung des Grundgesetzes folgend, für die Strafverfolgung eine Primärzuständigkeit der Länder vorsieht (§ 1 Abs. 3 BKAG) und deshalb eine direkte Zuständigkeit des BKA als Bundesbehörde lediglich als Ausnahme anzusehen ist. Vor diesem Hintergrund ist auch die Durchbrechung der Ausnahme in § 4 Abs. 2 BKAG restriktiv zu interpretieren. Auf der anderen Seite zwingen die datenschutzrechtlichen Grundsätze, amtshilferechtliche Vorschriften restriktiv zu interpretieren, da diese insbesondere nicht zum pauschalen Austausch von Eingriffsbefugnissen führen dürfen.[37] Hier ist allerdings zu berücksichtigen, dass sich die beteiligten Behörden insofern auf dieselbe Eingriffsgrundlage stützen (§ 100a StPO), es insofern jedenfalls

[36] Ahlf/Daub/Lersch/Störzer, BKAG, § 4 Rn. 18.
[37] vgl. ausführlich Schlink NVwZ 1986, 249, 251

nicht zur Befugniserweiterung kommt. Insofern spricht vieles dafür, die Regelung des § 4 Abs. 2 Satz 1 Nr. 1 BKAG insoweit nicht als abschließend anzusehen und deshalb als „Minus" die Zuständigkeit des BKA für einzelne Ermittlungshandlungen im Ersuchen der Landesbehörde auf diese Vorschrift zu stützen. Die Übermittlung der mit der Quellen-TKÜ erhobenen Daten kann das BKA (nur) auf die Generalermächtigung nach § 10 Abs. 1 BKAG stützen.

6. Schutz des Kernbereichs privater Lebensgestaltung

Zum Schutz des Kernbereichs privater Lebensgestaltung ist bei Maßnahmen der Telekommunikationsüberwachung ein zweifach gestufter Schutz zu gewährleisten.

Auf der ersten Stufe hat die Erhebung von Inhaltsdaten zu unterbleiben, wenn diese den Kernbereich privater Lebensgestaltung betreffen. Das Bundesverfassungsgericht ging ursprünglich davon aus, dass Gespräche in der Regel durch eine Gemengelage unterschiedlicher Inhalte geprägt sind.[38] Ein Überwachungsverbot, das erst eingreift, wenn sämtliche Erkenntnisse einem Verwertungsverbot unterliegen würden, sei unzureichend. Denn dies würde dazu führen, dass ein Überwachungsverbot selbst dann, wenn der Beschuldigte allein mit engsten Vertrauten kommuniziere, „praktisch niemals anzunehmen" sei. Diese Rechtsprechung hat das Bundesverfassungsgericht zumindest in Bezug auf die Telekommunikationsüberwachung mit seiner Entscheidung vom 12. Oktober 2011 nun wieder eingeschränkt.[39] Es hat dabei die Regelung des § 100a Abs. 4 StPO zum Kernbereichsschutz für die strafprozessuale Telekommunikationsüberwachung für verfassungskonform erachtet, nach der auf der Erhebungsebene eine Überwachung erst dann unzulässig ist, wenn diese „allein" den Kernbereich privater Lebensgestaltung berührt. „Ein ausschließlicher Kernbereichsbezug kann vor allem dann angenommen werden, wenn der Betroffene mit Personen kommuniziert, zu denen er in einem besonderen, den Kernbereich betreffenden Vertrauensverhältnis - wie zum Beispiel engsten Familienangehörigen, Geistlichen, Telefonseelsorgern, Strafverteidigern oder im Einzelfall auch Ärzten - steht (vgl. BVerfGE 109, 279 <321 ff.>). Soweit ein derartiges Vertrauensverhältnis für Ermittlungsbehörden erkennbar ist, dürfen Maßnahmen der Telekommunikationsüberwachung nicht durchgeführt werden."[40]

Diese Einschränkungen des Kernbereichsschutzes hat das Bundesverfassungsgericht aber mit dem notwendigen Schutz in der Auswertungsphase kompensiert, der auf der zweiten Stufe sicherzustellen ist. Dieser Schutz ist durch das in § 100a Abs.

---

[38] BVerfGE 109, 279, 330.
[39] BVerfG, Beschl. v. 12.10.2011, 2 BvR 236/08, Abs.-Nr. 213 ff., www.bverfg.de
[40] BVerfG, Beschl. v. 12. Oktober 2011, 2 BvR 236/08, Abs. Nr. 215.

4 Satz 2 StPO normierte Verwertungsverbot sowie das unverzügliche Löschungsgebot gewährleistet.[41] Für den Bereich der Gefahrenabwehr ergibt sich dies aus § 20l Abs. 6 BKAG bzw. aus § 23a Abs. 4a ZFdG.

Zu den Maßnahmen, bei denen Gespräche ausgeleitet wurden, haben meine Mitarbeiter die Gesprächsprotokolle darauf durchgesehen, ob diese kernbereichsrelevant waren.

Zur Entfaltung der Persönlichkeit im Kernbereich privater Lebensgestaltung gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen.[42] Vom Schutz umfasst sind auch Gefühlsäußerungen, Äußerungen des unbewussten Erlebens sowie Ausdrucksformen der Sexualität (a.a.O.).

In einem Verfahren des BKA (siehe oben B.I.6.) haben meine Mitarbeiter entsprechende Inhalte vorgefunden. Es handelte sich um Gespräche zwischen dem Beschuldigten und seiner Freundin in Südamerika, mit der dieser offenbar eine intime Beziehung pflegte. Erfasst wurden dabei insbesondere sexuelle Handlungen, die während des Gesprächs stattfanden. Dies lässt sich mühelos unter den Kernbereich privater Lebensgestaltung subsumieren.

Keine Bewertung kann ich hinsichtlich der Frage vornehmen, ob die Überwachung von vornherein hätte unterbleiben müssen, da sie die Kommunikation zwischen dem Beschuldigten und seiner Freundin betraf, mit der dieser eine intime Beziehung pflegte. Denn es ist davon auszugehen, dass bereits das anordnende Gericht im Vorfeld der Überwachung dieser Frage nachgegangen ist und diese in seiner Entscheidung berücksichtigt hat. „Durch die Vorbefassung eines Richters bei der Überwachung der Telekommunikationsüberwachung ist somit sichergestellt, dass der Kernbereichsschutz bereits im Vorfeld von einer unabhängigen Instanz in den Blick genommen wird und Beachtung findet."[43]

Nach Auskunft des BKA waren die Gesprächsaufzeichnungen auf Weisung der Staatsanwaltschaft nicht gelöscht worden. Die Staatsanwaltschaft habe dies allerdings deshalb so entschieden, weil eine sequenzielle Löschung nicht möglich gewesen sei. Die Entscheidung, die Daten nicht zu löschen, habe ich nicht zu bewerten, da ich für die Staatsanwaltschaft eines Landes nicht kontrollbefugt bin. Ich beabsich-

[41] BVerfG a.a.O., Abs. Nr. 220.
[42] BVerfGE 109, 279, 313.
[43] BVerfG, Beschl. v. 12. Oktober 2011, Abs. Nr. 223.

tige insoweit, den Sachverhalt an den zuständigen Landesbeauftragten für den Datenschutz weiterzugeben.

Allerdings tritt in dem konkreten Fall ein struktureller Mangel zu Tage. Nach Darstellung sowohl des BKA als auch des ZKA ist es in Fällen der „normalen" Telekommunikationsüberwachung technisch unproblematisch, auch Teile der Gesprächsaufzeichnungen zu löschen (nach Zeitabschnitten), soweit diese den Kernbereich privater Lebensgestaltung betreffen. Bei der Quellen-TKÜ sei eine entsprechende Funktion von DigiTask in Gesprächen angefordert, aber (noch) nicht realisiert worden. Es wurden keine Möglichkeiten implementiert, kernbereichsrelevante Teile von Gesprächen oder Chats gezielt zu löschen. Es können bei Gesprächen nur die ganzen Gespräche und bei Chats nur ganze Sitzungen gelöscht werden. Beim Löschen einer Sitzung wären ggf. auch Gespräche betroffen. Dies hat dazu geführt, dass kernbereichsrelevante Inhalte überhaupt nicht gelöscht wurden.

In allgemeiner datenschutzpolitischer Hinsicht möchte ich noch folgendes hinzufügen: Die Regelungen zum Kernbereichsschutz bei der Telekommunikationsüberwachung nach § 20l Abs. 6 BKAG, nach § 23a Abs. 4a ZFdG bzw. nach § 100a Abs. 4 StPO sind weniger weitreichend ausgestaltet, wie dies etwa für den Bereich des verdeckten Eingriffs in informationstechnische Systeme nach § 20k Abs. 7 BKAG der Fall ist. Bei der sog. Online-Durchsuchung sind sämtliche erhobenen Daten unter Sachleitung des zuständigen Gerichts vom behördlichen Datenschutzbeauftragten auf kernbereichsrelevante Inhalte durchzusehen. Für den Bereich der TKÜ fehlt eine solche Regelung, weshalb es zunächst auf die Beurteilung durch die ermittelnde Organisationseinheit und die Staatsanwaltschaft ankommt. Dies wurde zwar in der Entscheidung des Bundesverfassungsgerichts vom 12. Oktober 2011 im Grundsatz mit Verweis auf die Möglichkeiten nachträglichen Rechtsschutzes (§ 101 Abs. 7 Satz 2 bis 7 StPO) akzeptiert. Der vorliegende Fall zeigt jedoch, dass im Hinblick auf den Kernbereich privater Lebensgestaltung auch in der Praxis ein unterschiedliches Schutzniveau anzutreffen ist.

Hervorzuheben ist, dass das Bundeskriminalamt aktuell in Zusammenarbeit mit dem GBA eine Arbeitshilfe erstellt hat, wie der Schutz des Kernbereichs privater Lebensgestaltung in der Praxis sicherzustellen ist. Darüber hinaus hat das BKA Maßnahmen zur Fortbildung von „Kernbereichsbeauftragten" getroffen, die in den jeweiligen Organisationseinheiten bei Maßnahmen der Telekommunikationsüberwachung die Durchsicht der Gesprächsaufzeichnungen auf kernbereichsrelevanten Inhalte übernehmen.

Im Falle des ZKA besteht noch die Besonderheit, dass die Daten mehrfach gespeichert werden und eine Löschung einzelner Gespräche nur in zwei von vier Systemen gezielt durchführbar ist. Insofern wäre eine Löschung kernbereichsrelevanter Gespräche nicht durchführbar.

Unabhängig davon halte ich es für unabdingbar sicherzustellen, dass bei der Quellen-TKÜ nur solche Software eingesetzt wird, bei der eine gezielte und sichere Löschung von Gesprächsinhalten möglich ist.

7. Löschung der Überwachungssoftware

Gemäß § 20k Abs. 2 Satz 2 BKAG sind die mit der Installation der Überwachungssoftware am Zielsystem vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig zu machen. Für den Bereich der strafprozessualen Telekommunikationsüberwachung nach § 100a StPO bzw. für den spezifischen Anwendungsbereich des § 23a ZfdG fehlen entsprechende Regelungen. Dies führt zu besonderen Problemen, weil gerade in diesem Bereich die Beweissicherheit von hoher Bedeutung ist.

Problematisch ist dabei die Frage, wann und wie die Löschung erfolgt: Vor einer forensischen Untersuchung, wie anlässlich des Besuches beim BKA bekannt wurde oder erst nach der forensischen Untersuchung? Jeder Eingriff – auch die Löschung der Software ist ein Eingriff – führt nämlich zu Änderungen in verschiedenen Systemdateien und kann das forensische Untersuchungsergebnis beeinflussen.

Es entspricht daher den Grundsätzen der forensischen Beweissicherung, dass vor jeder forensischen Untersuchung eine Kopie des sichergestellten Datenträgers erstellt wird und die Untersuchung nur an dieser Kopie vorgenommen werden, um jede Veränderung des Originalasservats zu verhindern.[44]

Aus datenschutzrechtlicher Sicht ist dies ebenfalls problematisch. Denn der Zustand des Rechners zum Zeitpunkt der Sicherstellung wird als Beweismittel für oder gegen den Betroffenen verwendet, ist also in seiner Gesamtheit ein personenbezogenes Datum, das ihm zugerechnet wird. Jede Beeinflussung kann zur Unrichtigkeit führen. Gerade wenn es um die Frage geht, ob bestimmte Datenflüsse dem Betroffenen zuzurechnen sind oder sogar durch die Überwachungssoftware – ggf. versehentlich – ausgelöst wurden, kann ein ggf. vom Gericht bestellter Sachverständiger dies nach

[44] vgl. Widmaier, Anwaltshandbuch Strafverteidigung, 1. Aufl. 2006, Rn. 32 ff.; vgl. auch Bär, Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007, Rn. 432.

der Löschung nicht mehr prüfen. Die Löschungsverpflichtung des § 20k Abs. 2 BKAG gilt insofern nach ihrem Sinn und Zweck für ein laufendes System des Betroffenen, der vor einer unzulässigen Überwachung geschützt werden soll.

D. Nachrichtendienste des Bundes

Sofern und soweit vom Bundesamt für Verfassungsschutz (BfV) Beschränkungen i.S.d. § 3 G10 im Wege der sog. Quellen-Telekommunikationsüberwachung durchgeführt wurden, unterliegt dies nicht meiner Kontrollbefugnis. Diese ist gemäß § 24 Abs. 2 Satz 3 BDSG beschränkt, soweit die Maßnahme der Kontrolle der Kommission nach § 15 des Artikel 10-Gesetzes unterliegt.