Deutscher Bundestag **Drucksache 17/8544 (neu)**

17. Wahlperiode 06. 02. 2012

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Jan Korte, Herbert Behrens, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 17/8257 –

Computergestützte Kriminaltechnik bei Polizeibehörden

Vorbemerkung der Fragesteller

Die Aufrüstung computergestützter Ermittlungsmethoden schreitet rasant voran. Die Anstrengungen auf Bundes- und Landesebene werden seit 2007 auch auf Ebene der Europäischen Union (EU) vorangetrieben: Auf Initiative des ehemaligen Bundesinnenministers Dr. Wolfgang Schäuble hatten sich einige europäische Innenminister in der sogenannten Future Group organisiert, um bei Weichenstellungen zukünftiger Polizeiarbeit mitzureden. Schon damals wurde von „gewaltigen Informationsmengen, die für öffentliche Sicherheitsorganisationen nützlich sein können“ orakelt: Der erwartete „Digitale Tsunami“ würde demnach verheißen, Milliarden elektronischer Geräte in Echtzeit zu verfolgen und Verhaltensmuster ihrer Nutzer und Nutzerinnen zu analysieren.

Die Proteste gegen die Naziaufmärsche in Dresden Anfang 2011 sorgten zudem für mehr Bewusstsein in Bezug auf die polizeiliche Nutzung von Daten aus der Funkzellenauswertung (FZA). Die Daten werden ebenfalls von einer Software aufbereitet und analysiert, bevor sie einer Software zur Auswertung zugeführt werden. Diese in Polizeikreisen sogenannte telekommunikative Spurensuche kann aber auch in Echtzeit genutzt werden, wie es bereits 2009 über eine Plattform von Nokia Siemens Networks im Iran berichtet wurde: Die staatlichen Milizen registrierten Spontanversammlungen über auffällig viele Mobiltelefone in Funkzellen. In Deutschland kommt hierzu ein sogenannter International Mobile Subscriber Identity (IMSI)-Catcher zur Anwendung, mit dem Standort- und Verbindungsdaten eines zuvor ermittelten Mobiltelefons innerhalb einer Funkzelle eingegrenzt wird (Bundestagsdrucksache 17/7652).

Neben der seit langem üblichen Vorgangsverwaltung setzen Polizeien Ermittlungssoftware ein, die Beziehungen unter polizeilichen Datensätzen finden soll. Aufgebohrt mit Zusatzmodulen werden etwa in der Anwendung rsCase der deutschen Firma rola Security weitere Datenquellen angeschlossen, GPS-Tracker eingebunden oder per Onlineschnittstelle Daten aus der Telekommunikationsüberwachung (TKÜ) eingespielt. Die Suche nach Auffälligkeiten wird als „Data Mining“ bezeichnet und soll einen Mehrwert aus bislang unstrukturierter Information verschaffen. Die Software-Industrie bietet statisti-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 2. Februar 2012 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

sche Verfahren für die Polizeiarbeit an, die mittels „vorausschauender Analyse“ Kriminalitätsmuster erkennen und sogar Straftaten vorhersehen will.

Auch das Internet wird mit IT-Anwendungen ausgeforscht. Telekommunikationsanbieter sind zur Zusammenarbeit mit Verfolgungsbehörden verpflichtet und müssen hierfür technische Standards für „Lawful Interception“ (etwa: behördliches Abhören) einhalten. Von den Providern herausgegebene Daten werden automatisiert übertragen und ausgewertet. Weil immer mehr Nutzer und Nutzerinnen allerdings ihre Kommunikation verschlüsseln, infiltrieren Polizeien und Geheimdienste die genutzten Rechner direkt mittels staatlichen Trojanern. Auch die hierüber erlangten Rohdaten werden mittels Software automatisiert ausgewertet.

Die Überwachung des Nutzerverhaltens im Internet bleibt indes nicht auf den eigenen Rechner beschränkt. Soziale Netzwerke müssen ebenfalls Daten an Verfolgungsbehörden herausgeben. Zudem können die von den Nutzern angelegten Profile auch ohne richterlichen Beschluss computergestützt durchforstet werden. Auch in Blogs und Chaträumen kann nach Verhaltensanomalien, Interessen von Gruppen, Trends oder anderen Aussagen über Beziehungen zwischen Personen und Vorgängen gesucht werden.

Die Menge an Daten aus Videoüberwachung, Funkzellenauswertung, Peilsendern oder auch der Auswertung des Internets erfordert nicht nur gehörige Investitionen in breitbandige Netzwerke, Endgeräte oder Speichermedien. Vielfach laufen die Information in Lagezentren zusammen. Zur Visualisierung eingehender Informationen sollen Monitoring Centres den Behörden ein umfassendes Lagebild verschaffen und die Entscheidungsfindung und Führungsfähigkeit verbessern.

Die polizeilichen Begehrlichkeiten nach digitalen Kriminalwerkzeugen sind längst nicht gestillt. Dass stets nach neuen auszuspähenden Kommunikationsmitteln gesucht wird, belegt der kürzlich geleakte „Leitfaden zum Datenzugriff“ der Staatsanwaltschaft München (www.vorratsdatenspeicherung.de/images/leitfaden_datenzugriff_voll.pdf). Demnach nutzen die Behörden neben „Stillen SMS“ und IMSI-Catchern zum Lokalisieren von Mobiltelefonen auch das „eTicketing“ der Deutschen Bahn, um Verdächtige auszuspähen.

Um überhaupt einen Überblick zu kriminalistisch genutzter Digitaltechnik zu erlangen, ist ein Einblick in die Funktionsweise obligatorisch. Hierzu muss die Öffentlichkeit auch über deren Hersteller informiert sein. Sofern Daten verarbeitet werden, die tief in die Privatsphäre eingreifen oder Anwendungen sogar auf deren Grundlage Risikoanalysen erstellen wollen, muss zudem der Quellcode der Software offen gelegt werden. Diesen unter Verweis auf geschützte „Vermögenswerte“ der Hersteller zu verweigern (vgl. Bundestagdrucksache 17/7760), wird von dem Fragesteller nicht hingenommen.

Vorbemerkung der Bundesregierung

Einstufung als Verschlusssache „VS – geheim“

Die Informationen, die in den Antworten zu den Fragen 4a, 4b, 5a, 5b, 5c, 5d, 8, 10, 10b, 11a, 11b, 12a, 12b, 12c, 12d, 12e, 13, 13e, 16, 18e, 19j, 20b, 20c, 24, 24a, 24b, 25b, 25c, 25d, 25e und 25f enthalten sind, sind geheimhaltungsbedürftig und wurden von den Verfassern daher mit dem Geheimhaltungsgrad „GEHEIM“ eingestuft, da durch das Bekanntwerden dieser Information das Staatswohl gefährdet werden könnte oder den Interessen der Bundesrepublik Deutschland oder eines der Länder schwerer Schaden zugefügt werden kann.

Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei könnte die Gefahr entstehen, dass ihre operativen Fähigkeiten und

Methoden aufgeklärt würden. Dies gilt umso mehr, da sich einzelne Fragestellungen nicht auf die Fähigkeiten der Polizeibehörden beschränken. Durch die detaillierte Kenntnis über die Durchführung derartiger Maßnahmen durch das Bundesamt für Verfassungsschutz (BfV), den Bundesnachrichtendienst (BND) und den Militärischen Abschirmdienst (MAD) würde die Möglichkeit gegeben, aus den Informationen Rückschlüsse auf die Nutzungsmöglichkeiten des Mittels und damit mittelbar auf die Arbeitsweise der Nachrichtendienste zu gewinnen. Dass dies nicht geschieht, muss zum Schutz der Arbeitsfähigkeit und der Aufgabenerfüllung der Sicherheitsbehörden – und damit mittelbar zum Schutz der Sicherheit der Bundesrepublik Deutschland – sichergestellt bleiben.

Daher muss bei der Beantwortung dieser Anfrage eine Abwägung der verfassungsrechtlich garantierten Informationsrechte des Deutschen Bundestages und seiner Abgeordneten einerseits mit den dargestellten negativen Folgen für die künftige Arbeitsfähigkeit und Aufgabenerfüllung der Nachrichtendienste sowie der daraus resultierenden Gefährdung der Sicherheit der Bundesrepublik Deutschland erfolgen. Bezogen auf die vorgenannten Fragen führt die gebotene Abwägung zum Vorrang der Geheimhaltungsinteressen. Zur Wahrung der Informationsrechte der Abgeordneten wird auf die Hinterlegung einer ergänzenden, GEHEIM eingestuften Antwort (Anlage 1) in der Geheimschutzstelle des Deutschen Bundestages verwiesen. Die Tatsache, dass die Antworten auf die genannten Fragen bei der Geheimschutzstelle des Deutschen Bundestages hinterlegt sind, stellt keinen Hinweis darauf dar, ob die der Fragenstellung zugrundeliegenden Annahmen zutreffend sind.

1. Welche gesetzlichen Regelungen gelten für in Deutschland ansässige Telekommunikationsfirmen, Netzbetreiber und Serviceanbieter hinsichtlich der Überwachung von Telekommunikation?

Die Überwachung der Telekommunikation ist in den §§ 100a, 100b der Strafprozessordnung (StPO), den §§ 1, 3, 5 und 8 des Artikel-10-Gesetzes, den §§ 23a bis 23c und 23e des Zollfahndungsdienstgesetzes (ZFdG), § 20l des Bundeskriminalamtgesetzes (BKAG) sowie im Landesrecht geregelt. Ergänzend dazu sind die organisatorischen und technischen Vorkehrungen, die die Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, für die Umsetzung angeordneter Maßnahmen zur Überwachung der Telekommunikation treffen müssen, durch § 110 des Telekommunikationsgesetzes (TKG) und die Telekommunikationsüberwachungsverordnung (TKÜV) geregelt.

a) Welche Behörden der Bundesregierung (auch des Verfassungsschutzes) beteiligen sich seit wann an der internationalen Arbeitsgruppe Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Requirements?

Die Bundesnetzagentur (BNetzA) beteiligt sich seit 1996 an dieser Arbeitsgruppe.

b) Welche Behörden der Bundesregierung (auch des Verfassungsschutzes) beteiligen sich an welchen anderen nationalen oder internationalen Arbeitsgruppen zu Standards für Lawful Interception (Standardisierungsgremien)?

Die BNetzA beteiligt sich an der Standardisierungsgruppe ETSI Technical Committee Lawful Interception (ETSI TCLI).

Der MAD nimmt auf Einladung der BNetzA an Sitzungen zur Fortschreibung von technischen und organisatorischen Standardisierungen im Bereich der Telekommunikationsüberwachung teil.

Das Zollkriminalamt (ZKA), das Bundeskriminalamt (BKA) und die Bundespolizei (BPOL) beteiligen sich national an der KomGÜT (Kommission Grundlagen der Überwachungstechnik).

Das ZKA beteiligt sich international an dem ETSI TCLI sowie an dem 3. Generation Partnership Project (3GPP).

Das BfV ist seit November 2003 Mitglied bei 3GPP und European Telecommunications Standards Institute (ETSI) und nimmt regelmäßig an Sitzungen der Arbeitsgruppe, die sich mit „Lawful Interception“ befasst, teil.

c) Mit Vertretern welcher deutscher Firmen arbeiten Bundesbehörden desweiteren bezüglich internationaler oder deutscher Standards für Lawful Interception zusammen?

Die BNetzA arbeitet mit allen nationalen Mitgliedern der verschiedenen Standardisierungsorganisationen im Rahmen dieser Tätigkeit zusammen. An den unter Frage 1b aufgeführten Standardisierungsprozessen sind auch regelmäßig die Verbände der sog. Verpflichteten und die Hersteller beteiligt. Im Bedarfsfall bindet die BNetzA die Bedarfsträger der Telekommunikationsüberwachung in diese Zusammenarbeit ein.

d) Mit dem Abhören welcher Technologien haben sich die oben genannten Treffen bzw. Arbeitsgruppen befasst?

Die behandelten Standardisierungsthemen umfassen weitgehend die in der TKÜV und der Technischen Richtlinie nach § 110 Absatz 3 TKG erfassten Technologien und Dienste, wie leitungs- und paketvermittelnde Netze (Festnetze und Mobilfunknetze) einschließlich Internetzugangsweg sowie E-Mail.

e) Welchen Bedarf sieht die Bundesregierung zur Ausgestaltung zukünftiger Werkzeuge zur Telekommunikationsüberwachung, und welche Prognosen bzw. Studien liegen hierfür vor?

Telekommunikation verlagert sich zunehmend ins Internet. Die Bundesregierung beobachtet die Entwicklung aufmerksam und wird zu gegebener Zeit prüfen, ob und welche Maßnahmen erforderlich sind.

2. Wie wird die deutsche Telekommunikationsüberwachungsverordnung von 2002 durch die Bundesbehörden konkret umgesetzt?

Die TKÜV vom 22. Januar 2002 ist am 9. November 2005 außer Kraft gesetzt worden. Die Verordnung richtete sich gemäß deren § 2 an die Betreiber von Telekommunikationsanlagen, mittels derer Telekommunikationsdienstleistungen für die Öffentlichkeit angeboten wurden, und wurde mithin nicht von Bundesbehörden umgesetzt.

Auch die derzeit gültige TKÜV vom 3. November 2005, durch die die in Rede stehende Verordnung vom 22. Januar 2002 ersetzt wurde, richtet sich nach deren § 3 an die Betreiber von Telekommunikationsanlagen, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, und wird mithin nicht von Bundesbehörden umgesetzt.

a) Welche Bundes- und Landesbehörden und gesetzgebende Körperschaften sind zur Ausführung von TKÜ berechtigt?

Nach § 100b Absatz 1 Satz 1 StPO darf die Überwachung der Telekommunikation zum Zweck der Strafverfolgung nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung nach § 100b Absatz 1 Satz 2 StPO auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Werktagen von dem Gericht bestätigt wird, tritt sie nach § 100b Absatz 1 Satz 3 StPO außer Kraft. Auf Grund der gerichtlichen oder im Eilfall staatsanwaltschaftlichen Anordnung hat nach § 100b Absatz 3 Satz 1 StPO jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft oder ihren im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Telekommunikationsüberwachung nach § 100a StPO zu ermöglichen. Die Vollstreckung gerichtlicher Anordnungen zur Überwachung der Telekommunikation obliegt im Übrigen gemäß § 36 Absatz 2 StPO der Staatsanwaltschaft, die das Erforderliche veranlasst.

In der Praxis wird die Überwachung der Telekommunikation nach der StPO auf Bundesebene von dem Zollfahndungsdienst (ZFD, bestehend aus ZKA und Zollfahndungsämtern), den Hauptzollämter mit dem Arbeitsbereich Finanzkontrolle Schwarzarbeit (FKS), dem BKA und der BPOL ausgeführt.

Gemäß Artikel-10-Gesetz sind das BfV, der MAD und der Bundesnachrichtendienst (BND) als Bundesbehörden zur Durchführung von Beschränkungsmaßnahmen (TKÜ) berechtigt.

Gemäß § 23a ZFdG ist das ZKA zur Durchführung von präventiven TKÜ-Maßnahmen berechtigt.

Das BKA ist zur Abwehr von Gefahren des internationalen Terrorismus gemäß § 4a BKAG bei Vorliegen der Voraussetzungen des § 20l BKAG zur Durchführung von präventiven TKÜ-Maßnahmen berechtigt.

Des Weiteren sind Landespolizeibehörden bzw. die Verfassungsschutzbehörden der Länder zur Ausführung von TKÜ-Maßnahmen berechtigt.

b) Welche weiteren berechtigten Stellen können derartige Überwachungsmaßnahmen beantragen oder erlassen?

Keine.

c) Welche Gerichtsbeschlüsse oder richterlichen Anordnungen sind für welche Maßnahmen jeweils erforderlich, bzw. in welchen Fällen reicht eine Anordnung durch die Staatsanwaltschaft oder einer anderen Behörde?

Beschränkungsmaßnahmen i. S. d. Artikel-10-Gesetzes auf Bundesebene werden aufgrund eines schriftlichen Antrags des jeweiligen Behördenleiters oder seines Stellvertreters durch das Bundesministerium des Innern schriftlich angeordnet. Die G10-Kommission ist monatlich über die angeordneten Beschränkungsmaßnahmen vor deren Vollzug zu unterrichten. Bei Gefahr im Verzuge kann das Bundesministerium des Innern den Vollzug der Beschränkungsmaßnahmen auch bereits vor der Unterrichtung der Kommission anordnen. Anordnungen, die die Kommission für unzulässig oder nicht notwendig erklärt, hat das zuständige Bundesministerium unverzüglich aufzuheben. In den Fällen des § 8 tritt die Anordnung außer Kraft, wenn sie nicht binnen drei Tagen vom Vorsitzenden oder seinem Stellvertreter bestätigt wird. Die Bestätigung der Kommission ist unverzüglich nachzuholen.

Anordnungen nach § 23a Absatz 1, 3 oder 4 ZFdG ergehen auf begründeten Antrag der Behördenleitung des Zollkriminalamts, bei deren Verhinderung von deren Stellvertretung, nach Zustimmung des Bundesministeriums der Finanzen durch das zuständige Landgericht. Bei Gefahr im Verzug kann die Anordnung vom Bundesministerium der Finanzen getroffen werden; sie tritt außer Kraft, wenn sie nicht binnen drei Tagen vom Landgericht bestätigt wird (§ 23b Absatz 1 Satz 1 und 2, § 23b Absatz 3 Satz 1 ZFdG).

Eine Maßnahme nach § 20l BKAG darf nur auf Antrag des Präsidenten des BKA oder seines Vertreters durch das zuständige Gericht angeordnet werden. Bei Gefahr im Verzuge kann die Anordnung durch den Präsidenten des BKA oder seinen Vertreter getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Im Übrigen wird auf die Antwort zu Frage 2a verwiesen.

d) Wie werden TKÜ-Maßnahmen auf Rechtsgrundlage der Strafprozessordnung von solchen zur Gefahrenabwehr voneinander abgegrenzt, bzw. welcher Unterschied ergibt sich hieraus für die Provider?

Mit Ausnahme unterschiedlicher Rechtsgrundlagen gibt es im Hinblick auf die Durchführung der TKÜ-Maßnahmen bei den berechtigten Stellen keinen Unterschied. Auch für die Betreiber von Telekommunikationsanlagen ergibt sich kein Unterschied bei der Umsetzung angeordneter Überwachungsmaßnahmen. Im Übrigen wird auf die Antwort zu Frage 2c verwiesen.

e) Welche Rechtsgrundlage bieten die Bestimmungen des BKA oder des Bundespolizeigesetzes (BPolG) für eine TKÜ-Anordnung zur Gefahrenabwehr?

Das BPolG enthält keine Befugnis für TKÜ-Maßnahmen zur Gefahrenabwehr. Im Übrigen wird auf die Antwort zu Frage 2a verwiesen.

3. Wie setzen sich die Kosten für eine Telekommunikationsüberwachung im Einzelfall zusammen?

Bei TKÜ-Maßnahmen entstehen sowohl der beauftragenden Stelle als auch der verpflichteten Stelle Kosten. Der beauftragenden Stelle entstehen üblicherweise Kosten für das eingesetzte Personal (Beantragung, Einrichtung, technische Administration und Auswertung der Maßnahmen) und die eingesetzte Technik (Lizenzkosten, Abschreibungskosten für Hard- und Software, Wartungs- und Instandhaltungskosten). Darüber hinaus entstehen Kosten für die Anmietung der Datenleitungen, die zur Übertragung der ausgeleiteten TKÜ-Daten von der verpflichteten Stelle an die beauftragende Stelle benötigt werden. Der verpflichteten Stelle entstehen üblicherweise Kosten für das Personal und für die vorzuhaltende Hard- und Software.

a) Welche Kosten entstanden den Referaten des Bundeskriminalamtes (BKA) Einsatz- und IT-Unterstützung (im Bereich Organisierte Kriminalität – OK), Einsatz- und IT-Unterstützung (beim Staatsschutz), TKÜ und Mobilfunkforensik in den letzten fünf Jahren im Rahmen von Abhörmaßnahmen, und wie standen diese im Verhältnis zum Gesamtetat?

Kostenpflichtige Abfragen aus den genannten Bereichen werden im Hinblick auf die beauftragenden Stellen (OK, Staatsschutz etc.) nicht gesondert statistisch erfasst. Eine Aufteilung der geleisteten Zahlungen ist daher nicht möglich.

Es können lediglich die Gesamtkosten für Auskunftsersuchen für TKÜ aufgeführt werden:

2007	244 650,40 €
2008	208 043,28 €
2009	182 624,91 €
2010	260 147,40 €
2011	396 176,48 €.

Die Ausgaben stehen in folgendem Verhältnis zum Etat der Abteilung IT, der für diese Kostenpositionen herangezogen wird:

Haushaltsjahr	Kostenanteil im Bereich TKÜ/Auskunftsersuchen
2007	0,47 % des Gesamtetats
2008	0,46 % des Gesamtetats
2009	0,47 % des Gesamtetats
2010	0,60 % des Gesamtetats
2011	1,11 % des Gesamtetats.

b) Mit welchen Interception Service Providern arbeiten Bundesbehörden zur Umsetzung von Lawful-Interception-Aufträgen zusammen?

Den Begriff „Interception Service Provider“ kennt das deutsche Recht nicht. TKÜ wird entsprechend der in Frage 2a angeführten Rechtsgrundlagen ausschließlich im Zusammenwirken mit den verpflichteten Stellen durchgeführt.

Auf Grund einer Anordnung nach § 100a StPO hat jeder, der Telekommunikationsdienste erbringt oder daran mitwirkt, dem Gericht, der Staatsanwaltschaft und ihrer im Polizeidienst tätigen Ermittlungspersonen (§ 152 des Gerichtsverfassungsgesetzes) die Maßnahmen nach § 100a StPO zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Ob und in welchem Umfang hierfür Vorkehrungen zu treffen sind, bestimmt sich nach § 110 TKG und der TKÜV. Bei Anordnungen im Bereich der präventiven TKÜ gelten analoge Vorschriften der einschlägigen Fachgesetze.

Gemäß § 110 Absatz 6 TKG ist jeder Betreiber einer Telekommunikationsanlage, der anderen im Rahmen seines Angebotes für die Öffentlichkeit Netzabschlusspunkte seiner Telekommunikationsanlage überlässt, verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderungen Netzabschlusspunkte für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen unverzüglich und vorrangig bereitzustellen.

c) Welche Dienste werden in diesem Falle über Interception Service Provider ausgelagert (etwa Mietgeräte und Leihausrüstungen, technischer Support oder Managed Services)?

Die zur TKÜ berechtigten Bundesbehörden betreiben die zur Überwachung der Telekommunikation notwendigen technischen Einrichtungen ausschließlich in eigener Verantwortung.

d) Ist es Bundesbehörden – wie vom Abhördienstleister Utimaco berichtet – technisch möglich, die Ausforschung etwa einer einzigen E-Mail oder einer bestimmten Absenderadresse in großen Internetknoten wie DE-CIX zu gewährleisten oder werden derartige Dienste an private Firmen ausgelagert?

Derartige Überwachungsansätze werden von Bundesbehörden nicht durchgeführt.

4. Welche digitalen Anwendungen zur Lawful Interception werden für leitungsvermittelnde Netze, paketvermittelnde Netze, Funknetze, Übertragungswege für teilnehmerbezogenen Internetzugriff und Breitbandkabelnetze durch Bundesbehörden bzw. die hierzu verpflichteten TKÜ-Provider jeweils genutzt?

Zur Beantwortung der Frage wird davon ausgegangen, dass der in der Fragestellung verwendete Begriff TKÜ-Provider denjenigen Betreiber von Telekommunikationsanlagen im Sinne der Antwort zu Frage 1 bezeichnen soll, der zur Vorhaltung von Überwachungstechnik verpflichtet ist.

a) Welche Hardware welcher Anbieter kommt hierfür seit wann zum Einsatz?

Die von TK-Unternehmen eingesetzte Hard- und Software wird in der Regel systemintegriert durch den Hersteller der TK-Anlage bereitgestellt. Im Bedarfsfall werden von den Betreibern der TK-Anlagen zum Teil Spezialfirmen zur Schnittstellenanpassung beauftragt.

Siehe hierzu auch die Ergänzungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[1]

b) Welche Software welcher Anbieter kommt hierfür seit wann zum Einsatz?

Auf die Antwort zu Frage 4a wird verwiesen.[2]

c) Welche Übergabeschnittstellen zu Providern werden betrieben bzw. genutzt?

Die Schnittstellen für die Übermittlung der zu überwachenden Telekommunikation vom jeweiligen Betreiber der Telekommunikationsanlage an die jeweils zur Überwachung berechtigte Stelle richten sich nach den Festlegungen in der Technischen Richtlinie nach § 110 Absatz 3 TKG. Die eingesetzten Übergabeschnittstellen entsprechen den Vorgaben der Technischen Richtlinie zur TKÜV (TR TKÜV).[3]

d) Welche Behörden betreiben Server zum Ausleiten bzw. Empfangen von Daten aus der TKÜ durch Provider?

Jede zur Überwachung der Telekommunikation berechtigte Stelle betreibt zum Empfang der an sie übermittelten Kopien der zu überwachenden Telekommunikation entsprechende technische Einrichtungen (Computersysteme).

Im Hinblick auf die zur TKÜ berechtigten Stellen des Bundes wird auf die Antwort zu Frage 2a verwiesen.

[1, 2] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

[3] Gültige Fassung Abl. BNetzA, Ausgabe 01/2012, S. 10, abrufbar unter www.bundesnetzagentur.de

e) In welchen Fällen wurden oder werden Daten auf Datenträgern, etwa USB-Sticks oder gebrannte Datenträger, weitergegeben, und wie ist das Procedere hierzu?

Zur Übergabe der Überwachungskopien kommen regelmäßig keine Datenträger für den Datenaustausch zwischen den Verpflichteten (§ 2 Nummer 16 TKÜV) und den berechtigten Stellen (§ 2 Nummer 3 TKÜV) zum Einsatz. Der Datenaustausch erfolgt über definierte IT-Schnittstellen.

Nach Abschluss von TKÜ-Maßnahmen oder zu weiteren Analyse- bzw. Auswertezwekken während einer TKÜ-Maßnahme werden auf Anforderung der zuständigen Staatsanwaltschaft oder der ermittlungsführenden Dienststelle Daten automatisiert aus der vorhandenen TKÜ-Anlagentechnik generiert und mittels Datenträger unter Verwendung eines Übergabeprotokolls durch die zuständige TKÜ-Servicedienststelle an anfordernde Behörde weitergegeben.

5. Wie ist rechtlich und technisch umgesetzt, dass eine Anfrage zur TKÜ in Echtzeit bei den Providern unverzüglich aktiviert wird?

Nach § 110 Absatz 1 Satz 1 Nummer 1 TKG i. V. m. § 5 Absatz 3 TKÜV muss der Betreiber der Telekommunikationsanlage eine Anordnung zur Überwachung der Telekommunikation unverzüglich eigenverantwortlich umsetzen. Dazu hat er nach § 6 Absatz 1 TKÜV seine Überwachungseinrichtungen so zu gestalten, dass er die Anordnung unverzüglich umsetzen kann. Die Einhaltung der zur Umsetzung dieser Anforderung erforderlichen technischen Voraussetzungen wird von der BNetzA im Rahmen des Nachweises nach § 110 Absatz 1 Satz 1 Nummer 3 und § 19 TKÜV überprüft.

a) Wie greifen Bundesbehörden in Echtzeit bzw. nahezu Echtzeit auf Informationen aus der TKÜ zu?

Nach einer Umsetzung und Aktivierung der Telekommunikationsüberwachungsmaßnahme durch den Verpflichteten leitet dieser die zu überwachende Telekommunikation zeitgleich an die Aufzeichnungseinrichtung der berechtigten Stelle aus. Die ermittlungsführenden Dienststellen greifen mittels einer entsprechenden Software (TKÜ-Applikation) ggf. in Echtzeit auf die angelieferten Informationen der verpflichteten Stellen zu den einzelnen Telekommunikationsüberwachungsmaßnahmen zu.

Siehe hierzu die ergänzenden Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[4]

b) Über welche Übertragungsverfahren wird eine Übermittlung in Echtzeit bewerkstelligt?

Die Übermittlung der Kopie der zu überwachenden Telekommunikation vom Betreiber der Telekommunikationsanlage zu der jeweils berechtigten Stelle erfolgt bei der Überwachung von Telefonanschlüssen über ISDN, in Fällen der Überwachung von reinen VoIP-Anschlüssen, beim Internetzugang sowie bei E-Mail über eine IP-basierte gesicherte Übertragungsmöglichkeit.

Siehe hierzu die ergänzenden Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[5]

[4, 5] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

c) Welche Hard- und Software welcher Hersteller kommt für die gesamte Echtzeitmaßnahme (auch für die Auswertung der Daten) auf den Seiten von Bundesbehörden jeweils zum Einsatz?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[6]

d) Wie viele Echtzeitüberwachungsaktivitäten der TKÜ können von den bei den Bundesbehörden genutzten Plattformen jeweils gleichzeitig verarbeitet werden?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[7]

6. Wie wird bei den genutzten technischen Anwendungen sichergestellt, dass sensible private Daten während der Übertragung zur ausforschenden Behörde geschützt werden, und welche Verschlüsselungsverfahren kommen hierbei zur Anwendung?

Die Kopie der zu überwachenden Telekommunikation, die der Betreiber der Telekommunikationsanlage an die zur Überwachung der Telekommunikation berechtigten Stellen übermittelt, wird gemäß § 14 Absatz 2 TKÜV in Verbindung mit der Technischen Richtlinie nach § 110 Absatz 3 TKG vor der Kenntnisnahme durch Unbefugte geschützt. Generell ist sichergestellt, dass diese Kopie nicht irrtümlich an einen Anschluss außerhalb der Gruppe der berechtigten Stellen (geschlossene Benutzergruppe zwischen berechtigten Stellen und Verpflichteten, unidirektionaler Verbindungsaufbau) übermittelt wird; zudem sind die Kopien bei einer IP-basierten Übermittlung durch den Einsatz von besonderer Verschlüsselungstechnik (BPN und IPSec via SINA-Technologie) gesichert.

Im BND ist durch verschiedene mehrstufige Verfahren der Schutz sensibler, privater Daten bei der Übertragung gewährleistet.

a) Welches private oder behördliche Personal ist dazu autorisiert, die im gesamten Prozess anfallenden Überwachungsdaten einzusehen?

Bei den berechtigten Stellen ist ein kleiner Personenkreis in der Lage, die im gesamten Überwachungsprozess anfallenden Überwachungsdaten einzusehen. Dieser ist generell sicherheitsüberprüft sowie teilweise speziell für G10-Maßnahmen verpflichtet. Bei diesem Personenkreis handelt es sich um Administratoren der TKÜ-Einrichtungen. Von dieser theoretischen Möglichkeit wird jedoch regelmäßig mangels fachlicher Notwendigkeit kein Gebrauch gemacht. Alle weiteren Zugangsmöglichkeiten zu den TKÜ-Daten sind über ein Rechte-/Rollenkonzept geregelt. Die TKÜ-Daten sind nur Personen der berechtigten Stellen zugänglich, sofern sie diesen Zugang zur Erfüllung ihrer Aufgaben benötigen.

Auf private Institutionen wird im Rahmen der Durchführung von TKÜ-Maßnahmen seitens der Bundesbehörden nicht zurückgegriffen.

[6, 7] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

b) Wie wedvrden TKÜ-Aktivitäten protokolliert und wo werden diese Protokolle abgelegt?

Die zur Vorhaltung von Überwachungstechnik verpflichteten Betreiber der Telekommunikationsanlagen haben gemäß § 16 TKÜV sämtliche Anwendungen ihrer Überwachungseinrichtungen automatisch und lückenlos zu protokollieren. Dabei sind zu protokollieren:

– die Referenznummer oder eine unternehmensinterne Bezeichnung der Maßnahme,

– die eingegebene zu überwachende Kennung, auf Grund derer die Überwachungseinrichtung die Überwachungskopie bereitstellt,

– die Zeitpunkte, zwischen denen die Überwachungseinrichtung die Telekommunikation erfasst,

– die Adresse (Rufnummer) des Anschlusses, an den die jeweilige Überwachungskopie übermittelt wird,

– ein Merkmal zur Erkennbarkeit der Person, die die vorgenannten Eingaben gemacht hat sowie

– Datum und Uhrzeit der Eingaben.

Die Protokolldaten sind so abzulegen, dass sie nicht nachträglich verändert werden können. Nach § 17 TKÜV sind die Protokolldaten spätestens alle drei Monate zu prüfen und es ist ein Prüfbericht an die BNetzA zu senden. Die Protokolldaten sind nach Ablauf von zwölf Monaten nach Versendung des Prüfberichts an die BNetzA zu löschen. Zusätzlich haben sowohl die BNetzA nach § 16 Absatz 4 TKÜV als auch die für die Kontrolle der Einhaltung der Vorschriften über den Schutz personenbezogener Daten zuständigen Behörden das Recht, die Protokolldaten zu prüfen.

Alle TKÜ-Aktivitäten bei den berechtigten Stellen im Zusammenhang mit der Aufzeichnung, Verarbeitung und Auswertung von Telekommunikationsüberwachungsdaten werden von der Anlagentechnik aufgezeichnet und in hierfür vorgesehenen Dateien gespeichert. Es ist zu unterscheiden zwischen der Protokollierung im Rahmen der Führung des TKÜ-Verfahrens und einer Protokollierung im Bereich der TKÜ-Systemumgebung.

G10-Beschränkungsmaßnahmen des BfV und des BND sind in den jeweiligen Anträgen, in den Anordnungen des BMI, in den Akten der G10-Kommission, in den gemäß den Vorgaben des G10 verarbeiteten G10-Meldungen sowie in den monatlichen Unterrichtungen der G10-Kommission nach § 15 Absatz 7 G10 und in den halbjährlichen Berichten an das Parlamentarische Kontrollgremium nach § 14 Absatz 1 G10 dokumentiert. Diese Dokumente werden bei den zuständigen Stellen abgelegt.

c) Wie wird vor der Inbetriebnahme von Anlagen neuer Telekommunikationsprovider eine Abnahme ihrer Überwachungsausrüstung gewährleistet?

Nach § 110 Absatz 1 Satz 1 Nummer 3 TKG hat derjenige, der eine Telekommunikationsanlage betreibt, mit der Telekommunikationsdienste für die Öffentlichkeit erbracht werden, der Bundesnetzagentur den unentgeltlichen Nachweis zu erbringen, dass seine technischen Einrichtungen und organisatorischen Vorkehrungen zur Umsetzung angeordneter Maßnahmen zur Überwachung der Telekommunikation mit den Vorschriften der TKÜV und der technischen Richtlinie nach § 110 Absatz 3 TKG übereinstimmen. Dazu hat er der BNetzA auch die Prüfung vor Ort zu ermöglichen.

d) Welche Bundes- und Landesbehörden sind zur Prüfung jener Anlagen autorisiert?

Ausschließlich die BNetzA ist hierzu autorisiert.

e) Wie wird es seitens der einsetzenden Polizeien oder Geheimdienste technisch bewerkstelligt, dass Überwachungsmaßnahmen für die Betroffenen nicht erkennbar sind?

Die Ausleitung der Kopie der zu überwachenden Telekommunikation ist – außer in Fällen der Quellen-TKÜ – Aufgabe des Betreibers der Telekommunikationsanlage. Dieser hat nach § 5 Absatz 4 TKÜV sicherzustellen, dass die technische Umsetzung von angeordneten Maßnahmen zur Überwachung der Telekommunikation weder von den an der Telekommunikation Beteiligten noch von Dritten feststellbar ist.

7. Welchen Inhalt hat eine Überwachungsverfügung an den Telekommunikationsanbieter, und auf welchem Wege wird diese zugestellt?

Nach § 100b Absatz 2 Satz 2 StPO sind in der gerichtlichen – oder bei Gefahr im Verzug staatsanwaltschaftlichen – Anordnung zur Überwachung der Telekommunikation anzugeben, erstens soweit möglich, der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet, zweitens die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist, sowie drittens Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes.

Dem TK-Anbieter kann eine mit Unterschrift und Dienstsiegel versehene Ausfertigung oder beglaubigte Abschrift der Überwachungsanordnung schriftlich oder vorab per Telefax übermittelt werden. Ausreichend ist auch die Übersendung einer Kopie der Anordnung auf gesichertem elektronischem Weg. Im Fall der Faxübermittlung muss jedoch nach § 12 Absatz 2 der TKÜV dem Verpflichteten binnen einer Woche nach der Übermittlung der Faxkopie das Original oder eine beglaubigte Abschrift vorgelegt werden.

Anordnungen im Rahmen der in der Antwort zu Frage 2a genannten gefahrenabwehrrechtlichen Befugnisse von Polizeibehörden des Bundes orientieren sich in Form, Inhalt und Übermittlungsverfahren an den Anordnungen gemäß § 100b StPO.

Eine an den nach § 2 G10 Verpflichteten gerichtete Anordnung enthält Name und Anschrift des nach § 2 G10 verpflichteten TK-Anbieters, die Anordnungsnummer, die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder die Kennung des Endgerätes, wenn diese allein diesem Endgerät zuzuordnen ist (IMEI[8]). Dem Verpflichteten wird die Anordnung in Papierform in einer versiegelten Kunststoffversandtasche per Kurierdienst zugestellt, bei Sofortanordnungen auch vorab per Fax übersandt.

a) Wie viele Anordnungen haben die Bundesbehörden in den Jahren 2010 und 2011 erlassen (bitte nach Monaten aufschlüsseln)?

Außer in den Eilfällen, für die die in den Antworten zu den Fragen 2a und 2c genannten gesonderte Regelungen gelten, werden Anordnungen, welche durch

[8] Die „International Mobile Equipment Identity“ (IMEI) ist ein eindeutiger 15-stelliger Code, anhand dessen jedes Mobiltelefon eindeutig identifiziert werden kann.

BKA, BPOL und die Behörden des Zolls ausgeführt werden, ausschließlich von den zuständigen Gerichten und nicht durch andere Bundesbehörden erlassen. Für Eilanordnungen, die regelmäßig durch ein Gericht im Nachgang zu bestätigen sind, wird keine gesonderte Statistik geführt.

Im Hinblick auf die Anzahl der Anordnungen gemäß § 100a StPO wird auf die vom Bundesamt für Justiz veröffentlichte Statistik (www.bundesjustizamt.de) gemäß § 100b Absatz 5 und 6 StPO verwiesen.

Das BKA hat im Rahmen der Aufgabenwahrnehmung nach § 4a BKAG seit 2009 insgesamt 300 TKÜ-Maßnahmen nach richterlicher Anordnung durchgeführt (Stand: 3. Januar 2012).

Anordnungen nach dem G10-Gesetz werden durch das Bundesministerium des Innern erlassen und müssen – ausgenommen die in der Antwort zu Frage 2c) genannten Eilfälle – vor deren Vollzug durch die G10-Kommission bestätigt werden. Für G10-Maßnahmen gilt: Für das Jahr 2009 wird auf den Bericht gemäß § 14 Absatz 1 Satz 2 G10 – Bundestagsdrucksache 17/549, S. 4 f. – verwiesen. Entsprechende Berichte für die Jahre 2010 und 2011 liegen noch nicht vor. Die Anzahl der Maßnahmen für das Jahr 2010 beträgt 72. Für das Jahr 2011 liegen derzeit noch keine Angaben vor.

b) In welcher Zeitspanne muss der Diensteanbieter auf eine Anordnung zur TKÜ reagieren?

Nach § 110 Absatz 1 Satz 1 Nummer 1 TKG muss der Betreiber der TK-Anlage eine Anordnung zur Überwachung der Telekommunikation unverzüglich umsetzen. Dazu hat er nach § 12 TKÜV sicherzustellen, dass er jederzeit telefonisch über das Vorliegen einer solchen Anordnung und die Dringlichkeit ihrer Umsetzung informiert werden sowie innerhalb seiner üblichen Geschäftszeiten eine Anordnung jederzeit entgegennehmen kann. Außerhalb seiner üblichen Geschäftszeiten muss er eine unverzügliche Entgegennahme der Anordnung sicherstellen, spätestens jedoch sechs Stunden nach der Benachrichtigung.

c) Welche Möglichkeit hat der Provider, sich gegen eine polizeiliche oder richterliche Anordnung auf Herausgabe von Daten zu wehren?

Derjenige, der Telekommunikationsdienste erbringt oder daran mitwirkt und eine gerichtliche Anordnung zur Überwachung der Telekommunikation nach § 100b Absatz 3 Satz 1 StPO umzusetzen hat, kann Beschwerde nach § 304 StPO erheben. Der Polizei bzw. den Ermittlungspersonen der Staatsanwaltschaft ist es – auch bei Gefahr im Verzug – gesetzlich nicht gestattet, eine strafprozessuale Überwachung der Telekommunikation anzuordnen, so dass insoweit ein Rechtsbehelf nicht in Betracht kommt.

Rechtsmittel gegen gerichtliche Anordnungen nach dem ZFdG sowie nach § 20l BKAG bestimmen sich nach dem Gesetz über Verfahren in Familiensachen und in Angelegenheiten der freiwilligen Gerichtsbarkeit – FamFG (§ 23b Absatz 3 Satz 3 ZFdG).

d) Wie viele entsprechende Anordnungen haben Provider in den letzten beiden Jahren zurückgewiesen (bitte für Facebook, Skype, Google+, Twitter, StudiVZ und Wer kennt wen gesondert ausweisen)?

Den Behörden der Zollverwaltung, dem BKA und der BPOL liegen keine statistischen Angaben über Zurückweisungen entsprechender Anordnungen durch die Provider vor. Insofern kann hierzu keine Aussage getroffen werden.

Im Zuständigkeitsbereich des Generalbundesanwalts beim Bundesgerichtshof, des MAD, des BND und des BfV hat es in den letzten beiden Jahren keine Fälle einer Zurückweisung gegeben.

e) Welche ausländischen Provider arbeiten in der Praxis hinsichtlich sogenannter emergency disclosure request gut mit den Bundesbehörden zusammen, wie es die bayerische Generalstaatsanwaltschaft im „Leitfaden zum Datenzugriff“ etwa für Google, YouTube, Skype, Microsoft berichtet?

Dem BfV, BKA, MAD, der BPOL und den Behörden der Zollverwaltung liegen hierzu keine Informationen vor. Das Verfahren „emergency disclosure request“ findet im BND keine Verwendung.

Soweit auf Grundlage richterlicher Anordnungen sowie entsprechender Übereinkommen Amts- bzw. Rechtshilfe zur Durchführung von TK-Überwachungsmaßnahmen in anderen Staaten beantragt wird, sind die dortigen Strafverfolgungsbehörden aufgefordert, die diesbezüglichen Kommunikationsinhalte den inländischen Strafverfolgungsbehörden zur Verfügung zu stellen.

Bei den Ermittlungsreferaten des Generalbundesanwalts hat es in der Vergangenheit keine direkte Zusammenarbeit mit ausländischen Providern unter Umgehung der Rechtshilfe gegeben. Der zitierte Leitfaden der Generalstaatsanwaltschaft München betrifft in seinem einschlägigen Teil ausschließlich präventive Polizeiarbeit.

8. Welche Anwendungen bevorraten Bundesbehörden zur Analyse von telekommunikativen Daten aus der FZA?

Vorbemerkung

Es wird davon ausgegangen, dass mit dem Begriff der Funkzellenauswertung die Abfrage und Analyse der Daten der über einen bestimmten Zeitraum in einer Funkzelle angemeldeten Mobilfunkendgeräte gemeint ist.

Siehe hierzu die ergänzenden Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[9]

a) Wie werden die Bestandsdaten nach einer FZA von Providern an Verfolgungsbehörden übermittelt, welche Schnittstellen existieren hierzu, und inwieweit ist dieser Vorgang bereits automatisiert?

Bestandsdatenauskünfte werden den Ermittlungsbehörden, soweit erforderlich, von den Telekommunikations-Diensteanbietern in dem automatisierten Verfahren nach § 112 TKG unter Einschaltung der BNetzA oder in direktem Kontakt in dem manuellen Auskunftsverfahren nach § 113 TKG erteilt.

b) Welche Software welcher Hersteller wird hierfür eingesetzt, über welche Funktionalitäten verfügen die Anwendungen, und auf welche Datenbanken oder sonstigen Informationen wird lesend oder schreibend zugegriffen?

Bei dem automatisierten Auskunftsverfahren nach § 112 TKG richten die Ermittlungsbehörden ihre Anfragen an die BNetzA, die ihrerseits Anfragen bei den von den Telekommunikations-Diensteanbietern nach § 112 TKG vorzuhal-

[9] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

tenden Kundendateien durchführt. Das Ergebnis der Anfrage wird anschließend der anfragenden Behörde mitgeteilt. Die Schnittstellen sind beschrieben in der „Beschreibung der Schnittstelle für den Datenaustausch für das Auskunftsersuchen nach § 90 TKG zwischen der Regulierungsbehörde und den Verpflichteten (SARV)“ und der „Beschreibung der Schnittstelle für den Datenaustausch für das Auskunftsersuchen nach § 90 TKG zwischen der Regulierungsbehörde und den berechtigten Stellen (SARS)“, beide herausgegeben im September 1997 vom Bundesamt für Post und Telekommunikation. Die Anwendung läuft bei der BNetzA auf einer gesonderten, von anderen Anwendungen vollständig getrennten Hardware mit eigens dafür entwikkelter Software. Für das manuelle Auskunftsverfahren, das direkt zwischen den anfrageberechtigten Stellen und den Telekommunikations-Diensteanbietern abgewickelt wird, enthält die Technische Richtlinie nach § 110 Absatz 3 TKG auf ETSI-Standards beruhende technische Festlegungen.

c) Welche Bundesbehörden sind an der kriminaltechnischen Nutzung von Daten aus dem Elektronischen-Ticket-System (e-Ticketing) der Deutschen Bahn interessiert, und welche Initiativen bzw. Treffen mit welchen Firmen haben hierzu bereits stattgefunden?

Ein Nutzungserfordernis hat sich für Bundesbehörden mit kriminaltechnischen Zuständigkeiten bisher nicht ergeben. Deshalb wurden auch keine Kontakte zu Firmen oder anderen Institutionen in diesem Zusammenhang aufgenommen.

9. Kann die Bundesregierung, obwohl sie keine Statistiken über die Anwendung der Funkzellenauswertung führen will, für ihre einzelnen Behörden zumindest Angaben über die ungefähre Größenordnung ihrer Anwendung in den letzten fünf Jahren (etwa 1 bis 10 pro Jahr, 50 bis 100 pro Jahr, über 100 pro Jahr) bzw. wenigstens Angaben zu besonderen Tatkomplexen der Vergangenheit machen, anhand derer das Verfahren von polizeilichen Ermittlungen, Antragsstellung durch die Staatsanwaltschaft, richterlichem Beschluss bis hin zur Ausführung und Auswertung der Funkzellenauswertung durch die Fragesteller und Fragestellerinnen nachvollzogen werden kann?

Durch den MAD und den BND werden keine Funkzellenabfragen durchgeführt.

Im BKA sind seit 2006 Funkzellenabfragen in einer Größenordnung von insgesamt ca. 50 bis 100 angefallen. Die Funkzellenabfragen erfolgen zu strafprozessualen oder gefahrenabwehrrechtlichen Zwecken gemäß § 100g StPO bzw. § 20m BKAG.

Funkzellenabfragen erfolgen im Aufgabenbereich der BPOL ausschließlich in der Sachleitungsbefugnis der zuständigen Justizbehörden der Länder. Angaben hierzu obliegen insofern den hierfür zuständigen Landesregierungen.

Im Jahr 2011 gestattete der Ermittlungsrichter dem Generalbundesanwalt beim Bundesgerichtshof neun Funkzellenabfragen (Januar: 1, Februar: 1, April: 4, Juni: 1, Oktober: 1, November:1). Entsprechende Datenauswertungen aus den Jahren 2007 bis 2010 liegen nicht vor, da Funkzellenabfragen nicht gesondert statistisch erfasst werden und die zu Grunde liegenden Daten bereits gelöscht worden sind. Funkzellenabfragen erfolgten beispielsweise im Zusammenhang mit den Ermittlungen gegen die Mitglieder der „Düsseldorfer Zelle“ (mutmaßliche Al-Qaida Mitglieder um A.-K.) sowie im Zusammenhang mit den Brandanschlägen auf die Deutsche Bahn ab dem 10. Oktober 2011 im Raum Berlin und Brandenburg.

Im Hinblick auf BfV und die Behörden der Zollverwaltung wird auf die die Ausführungen in der Anlage verwiesen, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.

10. Inwieweit sind Bundesbehörden in der Lage, WLAN-Netzwerke mittels W-LAN-Catchern zu überwachen?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[10]

a) Wie ist ihr Einsatz rechtlich geregelt?

Ein WLAN-Catcher erfasst die über ein WLAN geführte Kommunikation einschließlich der anfallenden verbindungsbegleitenden Daten. Insofern wird auf die in der Antwort zu Frage 2a angegebenen Rechtsgrundlagen zur Überwachung der Telekommunikation verwiesen. Für die Ermittlung des WLAN-Namens (Service Set Identifier – SSID) für Zwecke der Strafverfolgung können die allgemeinen Befugnisregelungen der §§ 161 und 163 StPO herangezogen werden.

b) Welche Produkte welcher Hersteller wurden hierfür bereits begutachtet, getestet oder kommen zur Anwendung?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[11]

c) Wie oft haben Bundesbehörden in den letzten fünf Jahren von derartigen Geräten Gebrauch gemacht?

Durch die Behörden der Zollverwaltung, das BfV, die BPOL, den BND und den MAD erfolgte kein Einsatz eines WLAN-Catchers.

Von 2007 bis 2011 kam der WLAN-Catcher des BKA insgesamt 16 mal zum Einsatz.

11. Welche Anwendungen bevorraten Bundesbehörden zum Versenden von Stillen SMS (im Polizeijargon Ortungsimpulse)?

a) Mit welchen Anwendungen (Hard- und Software) welcher Hersteller werden die Stillen SMS versandt?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[12]

b) Welche Landes- oder Bundesbehörden verfügen hierzu über (auch gemeinsam genutzte) SMS-Server?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[13]

[10, 11, 12, 13] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

c) Kann die Bundesregierung Angaben zu besonderen Tatkomplexen der Vergangenheit machen, anhand derer das Verfahren von polizeilichen Ermittlungen, Antragsstellung durch die Staatsanwaltschaft, richterlichem Beschluss bis hin zur Ausführung und Auswertung durch die Fragesteller und Fragestellerinnen nachvollzogen werden kann?

Das Instrument der sog. Stillen-SMS wird in der Praxis im Zusammenhang mit TKÜ-Maßnahmen nach den §§ 100a, 100b StPO eingesetzt. In diesen Fällen – z. B. mit dem Ziel der Ergreifung des Beschuldigten oder zur Feststellung von Strukturen und Hinwendungsorten – ist neben der für die Ermittlung erforderlichen Erhebung der Telekommunikationsinhalte einschließlich der näheren Umstände der Telekommunikation die Nutzung dieses Einsatzmittels angezeigt.

Bei der zuständigen Staatsanwaltschaft wird die Beantragung eines richterlichen Beschlusses zur Überwachung der Telekommunikation angeregt. Die Staatsanwaltschaft prüft sodann die Erforderlichkeit, die Verhältnismäßigkeit sowie die weiteren rechtlichen Voraussetzungen der angeregten Überwachungsmaßnahme und stellt bei Vorliegen aller Voraussetzungen einen entsprechenden Antrag bei dem zuständigen Gericht, welches nach eigenständiger vollumfänglicher Überprüfung der Sach- und Rechtslage entscheidet. Der Beschluss wird nachfolgend von den Strafverfolgungsbehörden an den oder die Netzbetreiber zur Ausleitung der im Beschluss genannten Verbindungsdaten weitergeleitet. Nach Umsetzung der Ausleitung und Einrichtung der entsprechenden Überwachungsmaßnahme erfolgt die Auswertung der aufgezeichneten Daten. Soweit erforderlich werden von der ermittelnden Polizeidienststelle in diesem Zusammenhang sog. Stille SMS nach gesonderter Rücksprache mit der zuständigen Staatsanwaltschaft an das Mobiltelefon des Beschuldigten gesandt und in einem zweiten Schritt die auf diese Weise beim Netzbetreiber erzeugten Verkehrs- bzw. Standortdaten erhoben.

d) Kann die Bundesregierung exemplarisch schildern, nach welchem Verfahren eine richterliche Anordnung zur TKÜ an den Provider, das Versenden einer Stillen SMS durch die Polizei oder den Geheimdienst, das Ausleiten von derart erzwungenen Standort- oder Bestandsdaten durch einen Provider, das polizeiliche Verarbeiten der erlangten Daten sowie das weitere Versenden Stiller SMS miteinander synchronisiert sind?

Auf die Antwort zu Frage 11c wird verwiesen.

e) Wie ist die Nutzung Stiller SMS rechtlich geregelt, und welche Position vertritt die Bundesregierung hinsichtlich der Frage, ob es sich dabei um einen Kommunikationsvorgang handelt?

Für die Erhebung der durch die „Stille SMS“ erzeugten Daten kommen für den Bereich der Strafverfolgung § 100g StPO sowie die §§ 100a, 100b StPO in Betracht. In der Praxis der Strafverfolgungsbehörden erfolgt die Erhebung der Daten im Rahmen von Telekommunikationsüberwachungsmaßnahmen nach den §§ 100a, 100b StPO. Der eigentliche Grundrechtseingriff erfolgt durch die Erhebung der Daten und steht ausweislich der vorgenannten Normen (außer bei Gefahr im Verzuge) unter Richtervorbehalt.

Das reine Absenden einer „Stillen SMS“ ist als isolierte, taktische Maßnahme gesetzlich nicht gesondert geregelt. Die Strafverfolgungsbehörden stützen sich nach Maßgabe der Erforderlichkeit bezüglich des Absendens auf die Erhebungsbefugnisnorm selbst in Verbindung mit den §§ 161, 163 StPO.

Im Bereich der Nachrichtendienste und der Polizeibehörden des Bundes sind die dem § 100g StPO entsprechenden Vorschriften die Folgenden: § 8a Absatz 2 Nummer 4 BVerfSchG, § 4a MADG i. V. m. § 8a Absatz 2 Nummer 4 BVerfSchG, § 2a BNDG i. V. m. § 8a Absatz 2 Nummer 4 BVerfSchG, § 20m BKAG sowie § 23g ZFdG.

f) Wie wird sich die Bundesregierung im Bundesrat positionieren, wenn die Entwicklung strengerer Kriterien für die Anordnung, Durchführung und Protokollierung zukünftiger Maßnahmen zur Funkzellenauswertung oder des Versendens Stiller SMS zur Debatte steht?

Das Land Sachsen hat im Bundesrat einen Antrag für eine Neuregelung der Funkzellenabfrage eingebracht, dieser wurde vom Bundesrat allerdings bislang weder beraten noch entschieden. Sollte der Bundesrat entsprechende Vorschläge vorlegen, wird die Bundesregierung diese prüfen.

g) Welche fachliche Beratung wird von den zuständigen Fachausschüssen des Bundesrates bei welchen Experten hierzu gegenwärtig eingeholt?

Auf die Antwort zu Frage 11f wird verwiesen.

12. Welche Bundesbehörden sind zur Nutzung sogenannter IMSI-Catcher berechtigt, und welche rechtlichen Vorgaben liegen dem zugrunde?

Die Strafverfolgungsbehörden dürfen im Rahmen ihrer repressiven Befugnis einen „IMSI-Catcher“ nach Maßgabe des § 100i StPO einsetzen. Gegenstand der Ermittlungen muss eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 StPO bezeichnete Straftat, sein. Durch den Verweis in § 100i Absatz 3 Satz 1 StPO auf § 100b Absatz 1 Satz 1 bis 3 StPO wird geregelt, dass der Einsatz des „IMSI-Catchers“ nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden darf, bei Gefahr im Verzug die Anordnung auch durch die Staatsanwaltschaft getroffen werden kann und die Anordnung der Staatsanwaltschaft außer Kraft tritt, soweit sie nicht binnen drei Werktagen von dem Gericht bestätigt wird. Weitere Voraussetzung ist u. a., dass die Anordnung schriftlich zu ergehen hat (§ 100i Absatz 3 Satz 1 StPO i. V. m. § 100b Absatz 2 Satz 1 StPO) und dass die auf Grund der Anordnung ergriffenen Maßnahmen unverzüglich zu beenden sind, wenn die Voraussetzungen der Anordnung nicht mehr vorliegen (§ 100i Absatz 3 Satz 1 StPO i. V. m. § 100b Absatz 4 Satz 1 StPO).

Gemäß § 4a BKAG in Verbindung mit § 20n BKAG kann das BKA einen „IMSI-Catcher“ auch für Zwecke der Gefahrenabwehr einsetzen. Auch hierfür ist grundsätzlich ein richterlicher Beschluss erforderlich. Bei Gefahr im Verzug kann die Anordnung gemäß § 20n Absatz 3, Seite 1 BKAG in Verbindung mit § 20l Absatz 3 BKAG durch den Präsidenten des BKA getroffen werden. Dieser Beschluss muss unverzüglich durch ein Gericht bestätigt werden. Soweit diese Eilanordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

Der MAD darf gemäß § 5 MADG i. V. m. § 9 Absatz 4 BVerfSchG „IMSI-Catcher“ nutzen.

Das BfV ist gemäß § 9 Absatz4 BVerfSchG zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer berechtigt.

Der BND ist gemäß § 3 BNDG i. V. m. § 9 Absatz 4 BVerfSchG zum Einsatz von „IMSI-Catchern“ befugt.

a) Welche Hersteller haben Bundesbehörden wann IMSI-Catcher geliefert, und wie wurde die Vergabe jeweils geregelt?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[14]

b) Wie viele IMSI-Catcher stehen Bundesbehörden zur Nutzung zur Verfügung, und welche Spezifikationen weisen die Geräte auf?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[15]

c) Welche Geräte wurden und werden Bundesbehörden innerhalb der letzten fünf Jahre leihweise überlassen bzw. geleast oder gemietet?

BKA, BPOL, BfV, MAD und die Behörden der Zollverwaltung haben innerhalb der letzten fünf Jahre keine Geräte ausgeliehen, geleast oder gemietet.

Siehe hierzu die ergänzenden Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[16]

d) Welche Kosten sind für die Beschaffung von IMSI-Catchern in den letzten fünf Jahren entstanden?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[17]

e) Welche Geräte wurden wann und aus welchen Gründen aus dem Bestand entfernt?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[18]

f) Inwiefern ist es möglich, mittels der Geräte die Kommunikation eines einzelnen Teilnehmers oder einer gesamten Funkzelle zu unterdrücken?

Mittels der von Bundesbehörden eingesetzten „IMSI-Catcher“ ist es theoretisch möglich, die Kommunikation einzelner Teilnehmer, jedoch nicht die einer gesamten Funkzelle zu unterdrücken. Die Unterdrückung der Kommunikation ist jedoch regelmäßig nicht Ziel der Maßnahme.

13. Inwieweit können Bundesbehörden GPS-Empfänger unter anderem in Mobiltelefonen oder Navigationsgeräten als Spähwerkzeuge nutzen?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[19]

a) Mit welchen Firmen arbeiten Bundesbehörden hinsichtlich Location-Based Service-Diensten zusammen, und welche Anwendungen werden hierfür genutzt?

Eine Zusammenarbeit mit Firmen hinsichtlich „LocationBasedService-Diensten“ hat seitens der betroffenen Bundesbehörden bisher nicht stattgefunden.

14, 15, 16, 17, 18, 19 Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

b) Wie ist die Herausgabe der sensiblen Standortdaten von Überwachten durch den privaten Diensteanbieter geregelt?

c) Welche technischen Möglichkeiten bevorraten Bundesbehörden zur Erlangung oder Herausgabe von Signalen jener GPS-Module, die serienmäßig in Mobiltelefonen eingebaut sind?

Auf die Antwort zu Frage 13a wird verwiesen.

d) Inwieweit könnten Mautdaten, die beim automatisierten Abrechnungssystem mittels GPS oder On Board Unit anfallen, technisch genutzt werden, und welche rechtlichen Hürden existieren hierzu?

Gemäß § 4 Absatz 2 und § 7 Absatz 2 des Autobahnmautgesetzes ist eine Nutzung von Mautdaten für Zwecke der Strafverfolgung und Gefahrenabwehr unzulässig.

e) Inwiefern sind Bundesbehörden technisch in der Lage, SIM-Module in Fahrzeugen (etwa Audi-Ortungsassistent Cobra, BMW-Assist/ConnectedDrive oder ähnliche Systeme bei Porsche, Renault und Opel) für polizeiliche Zwecke zu nutzen bzw. welche Überlegungen oder Anstrengungen wurden für eine zukünftige Nutzung unternommen?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[20]

14. Welche Software welcher Hersteller kommt bei Bundesbehörden zur kriminalpolizeilichen Vorgangsverwaltung und Fallbearbeitung zur Anwendung zur Anwendung (bitte nach Vorgangsbearbeitung, kriminalistische Fallbearbeitung aufschlüsseln)?

	Vorgangsbearbeitungssystem (VBS)	Kriminalpolizeiliches Fallbearbeitungssystem (FBS)
BPOL	„@rtus-Bund“ (Firma Dataport)	„b-case“ (rola Security Solutions)
BKA	Allgemein: „Eigenentwickeltes VBS“ Kriminaltechnisches Institut: „Kriminaltechnisches Informationssystem“ (KISS) und „Forensisches Informationssystem Handschriften“ (FISH) (Firma GFaI – Gesellschaft zur Förderung angewandter Informatik)	„rsCase“ (rola Security Solutions) „Inpol-Fall“ (Eigenentwicklung BKA)
FKS	„Programmunterstützung Finanzkontrolle Schwarzarbeit“ (ProFiS); Eigenentwicklung (s. a. Antwort zu Frage 15)	
ZFD		„INZOLL“ (Individualsoftware; entwickelt von der Firma T-Systems International GmbH)

[20] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

a) Auf welche Polizeidatenbanken oder sonstigen Informationen dürfen die Anwendungen zugreifen?

BPOL

Der Zugriff auf polizeiliche Datenbanken seitens des VBS und FBS erfolgt gemäß den jeweiligen Berechtigungskonzepten dieser Anwendungen. Zusätzlich muss der Benutzer über entsprechende Berechtigung in der Anwendung verfügen, auf die ein Zugriff erfolgen soll.

Aus VBS kann bei Vorliegen der entsprechenden Berechtigung auf Inpol-BPOL, Inpol-Zentral und das Schengener Informationssystem zugegriffen werden.

Aus FBS kann bei Vorliegen der entsprechenden Berechtigung auf Inpol-Fall zugegriffen werden.

BKA

Der Zugriff auf polizeiliche Datenbanken seitens des VBS und FBS erfolgt gemäß den jeweiligen Berechtigungskonzepten dieser Anwendungen. Zusätzlich muss der Benutzer über entsprechende Berechtigung in der Anwendung verfügen, auf die ein Zugriff erfolgen soll.

Aus VBS kann bei Vorliegen der entsprechenden Berechtigung auf Inpol-Zentral, Inpol-Fall und das Schengener Informationssystem zugegriffen werden. Mittels der Vorgangsbearbeitungssysteme KISS/FISH erfolgt kein Zugriff auf Polizeidatenbanken oder sonstige Anwendungen.

Aus dem Landesfallbearbeitungssystem b-case und dem Verbundfallbearbeitungssystem Inpol-Fall kann bei Vorliegen der entsprechenden Berechtigung auf spezifische Verfahren von Inpol-Fall zugegriffen werden.

Zoll

Die IT-Verfahren INZOLL und ProFiS verfügen nicht über Schnittstellen zu Polizei-datenbanken.

b) Welche Datenbanksysteme welcher Hersteller liegen den Anwendungen jeweils zugrunde?

Mit Ausnahme des Verfahrens FISH liegt allen Anwendungen das Datenbanksystem der Firma Oracle zugrunde. Für FISH kommt das Datenbanksystem ADABAS der Firma Software AG zum Einsatz.

c) Welche Zusatzmodule werden hierbei im Regel- oder Einzelfall von der Software eingebunden?

BPOL

Für VBS sind keine Zusatzmodule eingerichtet. Für FBS ist die Bund-Länder-Onlineschnittstelle (BLOS-Modul) sowie das Geografische Informationssystem des Systems rsCase eingerichtet.

BKA

Für VBS sind keine Zusatzmodule eingerichtet. In KISS/FISH sind keine Zusatzmodule eingebunden. In b-case sind grundsätzlich alle beschafften Module eingebunden.

Siehe hierzu auch ergänzend die Ausführungen zur Frage 20c in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.

Zoll

In INZOLL sind keine Zusatzmodule eingebunden. Im IT-Verfahren ProFiS ist als „Zusatzmodul“ die „Erhebungshilfe FKS“ der Deutschen Rentenversicherung Bund (DRV) eingebunden. Mittels der „Erhebungshilfe FKS“ werden vom Arbeitsbereich FKS Ermittlungsergebnisse aufbereitet und der DRV elektronisch zur weiteren Bearbeitung (Prüfung, Schadensberechnung, Erteilung von Beitragsbescheiden) übermittelt.

d) Inwieweit können auch GPS-Tracker eingebunden werden?

In keinem der Systeme ist eine Einbindung eines GPS-Trackers vorgesehen.

e) Wie werden TKÜ-Daten von Telekommunikationsprovidern in die Anwendungen eingespielt?

BPOL und BKA

Im VBS ist keine Einspielung von TKÜ-Daten vorgesehen. Auf Antrag der ermittlungsführenden Abteilung können über eine Schnittstelle TKÜ-Daten aus der TKÜ-Anlage an rsCase übertragen werden.

Zoll

Die Einspielung von TKÜ-Daten von Telekommunikationsprovidern in das Fallbearbeitungssystem INZOLL erfolgt entweder manuell oder mit Hilfe eines sog. „Object-Loaders“, der die manuelle Erfassung simuliert. Die Einspielung von TKÜ-Daten in ProFiS ist nicht möglich.

f) Inwieweit kann die genutzte Software einen Mehrwert aus bislang unstrukturierter Information finden?

BPOL

Eine Suche von unstrukturierten Datenbeständen in VBS und FBS ist nur mittels Volltextrecherche möglich.

BKA

Bei VBS, b-case und Inpol-Fall ist eine Suche in unstrukturierten Datenbeständen nur über Volltextrecherche möglich. Bei KISS/FISH ist eine Suche in unstrukturierten Datenbeständen nicht möglich.

Zoll

In INZOLL können grundsätzlich Datenbankabfragen anhand spezieller Suchkriterien durchgeführt werden. Der Mehrwert dieser Datenbankabfragen ist vom Einzelfall abhängig. Im IT-Verfahren ProFiS ist eine solche Abfrage nicht möglich.

15. Handelt es sich bei den Systemen zur Vorgangsverwaltung und Fallbearbeitung jeweils um Entwicklungen durch Dritte im Auftrag bzw. für den Einsatzzweck der jeweiligen Behörden, um die Beschaffung (und gegebenenfalls Anpassung) sogenannter Commercial off the shelf-Produkte (COTS) oder um Eigenentwicklungen der Behörden?

BPOL

Das VBS der Bundespolizei @rtus wird in einer Kooperation zwischen dem Land Schleswig-Holstein und dem Bund gemeinsam weiterentwickelt und gepflegt. Für die dafür erforderliche Programmierleistung beauftragt das Land

Schleswig-Holstein die Firma Dataport im Auftrag der Kooperation. Das FBS basiert auf dem Produkt rsCase der Firma rola Security Solution.

BKA

Bei VBS und FISH handelt es sich um Eigenentwicklungen, beim Fallbearbeitungs-system b-case um das Basisprodukt rsCase der Firma rola Security Solutions, welches BKA-spezifisch angepasst wurde. Das Verbundfallbearbeitungssystem Inpol-Fall ist eine Eigenentwicklung auf Basis von Crime. Bei KISS handelt es sich um eine Entwicklung durch Dritte (Firma GFaI) im Auftrag des Kriminaltechnischen Instituts (KTI) des BKA.

Zoll

INZOLL wurde durch einen externen Auftragnehmer im Auftrag des ZKA entwickelt. Im Arbeitsbereich FKS wurde mit Übergang der Verfolgungszuständigkeit für die Bekämpfung der Schwarzarbeit und der illegalen Beschäftigung im Bereich des Bundes zum 1. Januar 2004 auf die Zollverwaltung die bis dato von der Arbeitsverwaltung genutzte, auf Microsoft Access basierende Software (coLei-PC BillB), integriert. Die Software wurde auf eine ORACLE-Datenbank umgestellt und auf das Aufgabenprofil des Arbeitsbereiches FKS zugeschnitten. Die Anpassung des IT-Verfahrens wurde als Eigenentwicklung auch mit externer Unterstützung der Firma ORACLE umgesetzt. Das Frontend von ProFiS basiert weiterhin auf Microsoft Access.

a) Welche Kosten sind Bundesbehörden im Einzelfall und unter Berücksichtigung der Arbeitszeit innerhalb der Behörde für die Beschaffung, Anpassung, den Service und Pflege der Software bisher entstanden?

Vorbemerkung

Die Kosten für die Arbeitszeit von Mitarbeitern der Bundesbehörden können mangels hierzu geführter Statistiken nicht erhoben werden.

BPOL

Die Kosten für das VBS werden nicht gesondert erfasst. Eine Differenzierung der Allgemeinkosten war in der Kürze der Zeit nicht möglich gewesen. Eine konkrete Antwort zu dieser Teilfrage wird unaufgefordert bis zum 29. Februar 2012 nachgereicht. Die Kosten für das FBS belaufen sich auf 4 389 056,35 Euro (Stand: August 2011).

BPOL

Die Kosten im direkten Zusammenhang mit dem Vorgangsbearbeitungssystem artus-Bund belaufen sich in den Jahren

2009 auf 1 408 950,45 Euro

2010 auf 1 216 957,55 Euro und

2011 auf 933 392,85 Euro.

Diese Kosten beinhalten die jährlichen artus-Kooperationskosten, Entwicklungs-/Anpassungskosten für angeschlossene Systeme (z. B. artus-Recherche, elAn, modPKS etc.) sowie die Administrations- und Beratungskosten – insbesondere an die Dienstleister Dataport und T-Systems.

BKA

Für VBS sind in den letzten fünf Jahren ca. 8,6 Mio. Euro Ausgaben an Dritte erfolgt. Für b-case belaufen sich die Ausgaben an Dritte seit Ende 2005 auf ca. 4,7 Mio. Euro. Für Inpol-Fall wurden in den letzten vier Jahren für externe

Dienstleistungen zur Weiterentwicklung ca. 6,6 Mio. Euro verausgabt. Die Gesamtkosten für Beschaffung, Anpassung, Service und Pflege für das System KISS von 1998 bis heute betragen ca. 1 Mio. Euro.

Zoll

Für Entwicklung, Pflege und Betrieb von INZOLL sind in den letzten zehn Jahren insgesamt Kosten i. H. v. ca. 52,5 Mio. Euro entstanden. Die Weiterentwicklung, Wartung und Pflege des IT-Verfahrens ProFiS wird durch das Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) gewährleistet. Die Kosten hierfür werden für die letzten fünf Jahre auf ca. 3 Mio. Euro geschätzt.

b) Wurden für die Systeme bisher schon Wirtschaftlichkeitsbetrachtungen entsprechend den Empfehlungen des Beauftragten der Bundesregierung für Informationstechnik (CIO Bund) durchgeführt, und wenn ja, mit welchem Ergebnis, bzw. wenn nein, warum nicht?

BPOL

Für das Projekt PAVOS (Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem) wurde eine Wirtschaftlichkeitsbetrachtung erstellt, welche die Einführung eines VBS gestattete. Die durchgeführte Wirtschaftlichkeitsbetrachtung zum FBS (rsCase) bildete die Voraussetzung für die Beschaffung.

BKA

Für VBS wurde eine Wirtschaftlichkeitsbetrachtung gemäß WIBE 4.1 durchgeführt. Für b-case wurde ebenfalls eine Wirtschaftlichkeitsbetrachtung gemäß WIBE 4.1 durchgeführt. Für KISS wurde eine Wirtschaftlichkeitsbetrachtung gemäß WIBE 4.0 durchgeführt. Die Wirtschaftlichkeitsbetrachtungen bildeten jeweils die Voraussetzung für die Beschaffung/Eigenentwicklung.

Für Inpol-Fall wurde keine Wirtschaftlichkeitsbetrachtung durchgeführt, da die Einführung auf Basis der Überlassung eines Moduls der bereits vorhandenen POLAS Eigenentwicklung von HH und HE erfolgte.

Die Entwicklung von FISH erfolgte in den 70er- und 80er-Jahren, vor der Einführung der WIBE.

Zoll

Für INZOLL wurden Wirtschaftlichkeitsbetrachtungen entsprechend der Empfehlung zur Durchführung von Wirtschaftlichkeitsbetrachtungen in der Bundesverwaltung, insbesondere beim Einsatz der IT (Band 92) durchgeführt. Die durchgeführte Wirtschaftlichkeitsbetrachtung bildete die Voraussetzung für die Beschaffung.

Für das IT-Verfahren ProFiS wurde keine formalisierte Wirtschaftlichkeitsbetrachtung erstellt, da ein bestehendes Verfahren von der Arbeitsverwaltung übernommen und lediglich an die Erfordernisse der FKS angepasst worden ist (s. auch Antwort zu Frage 15).

16. Welches Volumen haben bzw. hatten Lizenz-, Support- und Serviceverträge von Bundesbehörden innerhalb der letzten fünf Jahre mit den Firmen Oracle, Microsoft (Datenbanksystem), Trivadis, Mummert & Partner, Gora. Hecken & Partner und der Valora Management Group?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[21]

[21] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

a) Welche Software der Firma IBM (bitte die Produktbezeichnung angeben) nutzt das BKA wie in der Antwort der Bundesregierung auf Bundestagsdrucksache 17/6587 berichtet „zu Testzwecken“, und welche „einzelfallabhängig unterschiedliche kriminalistische Fragestellungen“ wurden jeweils damit bearbeitet?

Das BKA beschaffte in 2010 zu Testzwecken die IBM-Software „InfoSphere Global Name Analytics“. Es fand kein kriminalistischer Einsatz statt.

b) Wer hat die Initiative zum Test der IBM-Anwendung ergriffen, und welche Kosten fielen für die Beschaffung an?

Die Initiative zum Test der IBM-Anwendung wurde seitens BKA ergriffen. Es fielen Kosten in Höhe von 85 975,12 Euro an.

c) Welche Firmen haben zusammen mit dem BKA im Rahmen der Spezialmesse General Police Equipment Exhibition & Conference 2010 in Leipzig an der Arbeitsgruppe Software-Koordinations-Maßnahmen im Bereich der IT-Forensik teilgenommen?

Das BKA nahm an der Arbeitsgruppe „Software-Koordinations-Maßnahmen im Bereich der IT-Forensik“ nicht teil. Die Teilnehmer der sind Bundesregierung nicht bekannt.

d) Welche Inhalte wurden in der Arbeitsgruppe Software-Koordinations-Maßnahmen im Bereich der IT-Forensik erörtert (bitte in groben Zügen wiedergeben)?

Die Themen, die in der Arbeitsgruppe erörtert wurden, sind dem BKA nicht bekannt. Im Übrigen wird auf die Antwort zu Frage 16c verwiesen.

17. Inwieweit unterscheiden sich beim Bundeskriminalamt Fallbearbeitungssysteme für die eigene operative Arbeit von jenen Anwendungen, die in seiner Rolle als Zentralstelle für kriminalpolizeiliche Informationssysteme für Bund und Länder genutzt werden?

Die Geschäftsprozesse/Anforderungen des BKA unterscheiden sich wegen der unterschiedlichen gesetzlichen Aufgaben von denjenigen der Polizeien der Länder. Dies hat u. a. Auswirkungen auf die Analysefunktionalitäten, Datenmengen, Performance, Datenmodelle usw., die im Rahmen der Erledigung von ausschließlich dem BKA zugeordneten Aufgaben bzw. im Rahmen der Erledigung von Aufgaben im Rahmen der Zentralstellenfunktion notwendig sind.

a) Seit wann existieren beim BKA die sogenannte Bund-Länder-Datei-Schnittstelle (BLDS) und die Bund-Länder-Online-Schnittstelle (BLOS)?

Die BLDS wurde 2006 im Rahmen der Vorbereitung auf die Fußball-Weltmeisterschaft 2006 in Deutschland entwickelt. Die BLOS steht seit Ende des Jahres 2007 zur Verfügung.

b) Worum handelt es sich bei diesen Schnittstellen, und wofür werden sie seit wann, und von wem genutzt?

Die BLDS erlaubt es den Inpol-Teilnehmern, im jeweiligen Landesbestand vorliegende, verbundrelevante Daten oder im Zusammenhang mit Großschadenslagen gewonnene Daten automatisiert an Inpol-Fall zu übertragen. Die BLDS-Schnittstelle kann durch jeden Inpol-Teilnehmer nach entsprechendem Freigabeverfahren genutzt werden.

Über die BLOS können Recherchen aus einem Fremdsystem an Inpol-Fall gestellt und das Ergebnis der Anfrage von Inpol-Fall an das Fremdsystem zurückübermittelt werden. Der Umfang der Nutzung wird durch den jeweiligen Inpol-Teilnehmer entsprechend der für ihn eingerichteten Rechte bestimmt.

c) Wer hat diese Schnittstellen entwickelt, und wie war das Beschaffungsverfahren für deren Entwicklung ausgestaltet?

Bei der BLDS und der BLOS handelt es sich um Eigenentwicklungen des BKA.

d) In welchem Umfang und für welche Zwecke werden das vom BKA im Rahmen seiner Zentralstellenfunktion gegenüber den Verbundteilnehmern zur Verfügung gestellte Informationssystem Inpol-Fall als Basis für den (derzeitigen) Kriminalpolizeilichen Meldedienst und die Anti-Terror-Datei sowie die BLDS und die BLOS von den Ländern und anderen Verbundteilnehmern im operativen Einsatz genutzt?

Das BKA stellt im Rahmen seiner Zentralstellenaufgabe die Verbundanwendung Inpol-Fall und die Schnittstellen BLDS und BLOS zur Verfügung. Die Verbundteilnehmer nutzen Inpol-Fall im Rahmen des vorgegebenen rechtlichen Rahmens. Inpol-Fall dient auch als Quellsystem für die Antiterrordatei.

e) Welche Firma oder Behörde hat die Datenbankstruktur von Inpol-Fall sowie die auf diese Datenbank zugreifende Erfassungs- und Abfragesoftware entwickelt bzw. an der Entwicklung mitgewirkt?

Bei Inpol-Fall handelt es sich um eine Weiterentwicklung auf Basis der Landesfallsoftware „Crime“ aus Hamburg und Hessen. Die Weiterentwicklung wurde durch das BKA selbst vorgenommen.

f) Wie und in welchem Umfang wurden die Nutzungs-, Bearbeitungs- und Verwertungsrechte des Vorgängersystems namens Crime von Inpol-Fall an das BKA übertragen, und wer war der übertragende Rechteinhaber?

Dem Bund wurde durch die Länder Hessen und Hamburg das räumlich, zeitlich und inhaltlich unbeschränkte Recht eingeräumt, die POLAS-Software inklusive des Moduls „Crime“ zu nutzen, zu verändern, zu bearbeiten, weiterzuentwickeln, zu dekompilieren, zu übersetzen oder auf andere Weise umzuarbeiten oder umarbeiten zu lassen.

18. Wie grenzt sich das System Inpol-Fall technisch und rechtlich ab von dem unter der Ägide des Inpol Land COmpetence Center (IPCC) bzw. der Hessischen Zentrale für Datenverarbeitung (HZD) weiterentwickelten und ebenfalls als Fallbearbeitungssystem angebotenen Systems Crime?

Bei dem Verbundsystem Inpol-Fall und dem Fallbearbeitungssystem „Crime“ handelt es sich um zwei eigenständige Entwicklungen, die auf derselben Software/Quellcode aus dem Jahr 2002 aufbauen. Seit 2002 wurden die beiden Systeme und ihr Quellcode unabhängig voneinander weiterentwickelt.

Beim Verbundsystem Inpol-Fall und dem Fallbearbeitungssystem „Crime“ handelt es sich zwischenzeitlich um zwei eigenständige, voneinander unabhängige Produkte.

a) Was hat die Bundesregierung unternommen, um zu prüfen, welche Synergieeffekte sich durch eine Zusammenlegung der Weiterentwicklung und Pflege der zwei sehr ähnlichen Systeme, Inpol-Fall und Crime, erzielen ließen, und welche Ergebnisse hat diese Prüfung ergeben?

Aus Sicht des BKA war aufgrund der besonderen Anforderungen an Verbunddateien, die im System Inpol-Fall betrieben werden (u. a. Besitzerprinzip, differenziertes Benutzerrechtekonzept, hohe Verfügbarkeit und Performanz bei großen Datenmengen), eine separate Entwicklung und Pflege der Systeme CRIME und Inpol-Fall erforderlich. Inzwischen unterscheiden sich die Systeme, trotz derselben Basis aus dem Jahre 2002, so stark im Quellcode, dass eine einheitliche Wartung und Pflege nicht wirtschaftlich wäre.

b) Stellt die generische Datenbankstruktur des Systems Inpol-Fall und seines Vorgängersystems Crime nach Ansicht der Bundesregierung eine Verletzung des Patents auf die Datenbankstruktur dar, die im System Polygon realisiert ist und im Besitz der Firma Polygon steht?

Die in Rede stehenden angeblichen Patentrechtsverletzungen zum Nachteil der Firma Polygon werden seit Jahren von dieser nicht nur gegenüber dem BKA, sondern auch gegenüber anderen Behörden vorgetragen. Sie wurden bisher weder hinreichend konkretisiert, noch erfolgreich erstritten.

c) Wie ist der aktuelle Stand der Planung bzw. Umsetzung zur Neuaufstellung des Kriminalpolizeilichen Meldedienstes auf der Basis des geplanten „Polizeilichen Informations- und Analyseverbunds für Bund und Länder (PIAV) (siehe Bundestagsdrucksache 17/5328)?

Die IMK hat in ihrer Herbstsitzung auf Vorschlag des AK II am 8./9. Dezember 2011 beschlossen, dass eine Einführung von PIAV geboten ist. Dazu wurde das BMI gebeten, in Abstimmung mit und unter Beteiligung der Länder eine Feinkonzeption zu erarbeiten. Die Erarbeitung der Feinkonzeption durch Bund und Länder, die im Laufe des Jahres 2012 der IMK vorgestellt werden soll, befindet sich derzeit in Umsetzung.

d) Welche konkreten technischen Prüfaufträge wurden erteilt, um die Möglichkeit zu untersuchen, das vorhandene System Inpol-Fall für die Zwecke von PIAV weiterzuentwickeln bzw. zu erweitern, und zu welchen Ergebnissen hinsichtlich der Machbarkeit, des Zeit- und Kostenaufwands sind diese Prüfungen gekommen?

Inpol-Fall wurde im Rahmen der Bund-Länder-Expertengruppe PIAV betrachtet. Für ein neues zukunftsweisendes PIAV-Zentralsystem kommt Inpol-Fall nach Einschätzung der Expertengruppen aufgrund bestehender funktionaler und technischer Einschränkungen nicht in Betracht.

e) Welche Rolle spielt bzw. spielte nach den Erkenntnissen der Bundesregierung die Gesellschaft für technische Sonderlösungen (GTS) bzw. deren Geschäftsführer als Anbieter bzw. Dienstleister auf dem Gebiet der Lawful Interception?

Im Jahr 2009 wurde durch BKA eine Lizenz für die Software „Netwitness“ als forensisches Analysewerkzeug zur Untersuchung von Netzwerkdaten erworben. Alleiniger Vertriebspartner in Deutschland für dieses Softwareprodukt und somit Ansprechpartner für das BKA war seinerzeit die Firma GTS in Person des Geschäftsführers, Felix J. Der Lizenzerwerb fand in der Folge unter Einbindung der Firma AIM GmbH statt. Die Software „Netwitness“ wurde und wird ausschließlich zur forensischen Untersuchung von bereits erhoben Netzwerkdaten, nicht zur Aufzeichnung solcher Daten, eingesetzt.

Siehe hierzu die ergänzenden Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[22]

f) War die Firma GTS oder ihre der Bundesregierung bekannte frühere Mitarbeiter und Mitarbeiterinnen mit der Entwicklung von Trojaner-Software des Bundes beauftragt bzw. daran beteiligt?

Weder die Firma GTS noch der Bundesregierung bekannte ehemalige Mitarbeiter waren an der Entwicklung von Remote Forensic Software (RFS) beteiligt. Es bestanden diesbezüglich keinerlei Kontakte zu der Firma.

19. Seit wann wird das Fallbearbeitungssystem der Firma rola Security beim BKA eingesetzt?

Das Fallbearbeitungssystem b-case der Firma rola Security Solutions wird seit dem Beginn des Probebetriebs am 22. Dezember 2005 im BKA eingesetzt.

a) Warum nutzt das BKA für die Fallbearbeitung, -analyse und -auswertung im Rahmen seiner eigenen, operativen Aufgaben ein Fallbearbeitungssystem auf der Basis von rsCase der Firma rola Security, und nicht das beim BKA für Zentralstellenaufgaben eingesetzte Informationssystem Inpol-Fall?

Es wird auf die Antwort der Bundesregierung zu Frage 3 auf die Kleine Anfrage der Fraktion DIE LINKE. „Lobbyismus bei Beschaffungsprojekten des Bundesministeriums des Innern“, Bundestagsdrucksache 17/5343 verwiesen.

b) Wird vom BKA auch die seitens rola beworbenen „automatische Erkennung und Darstellung vorhandener Strukturen zwischen Personen, Organisationen und gemeinsam verwendeter Infrastruktur“ genutzt?

Nein.

c) Welche Schnittstellen und Module können im Regel- sowie im Einzelfall eingebunden werden?

Prinzipiell können alle von der Firma rola Security Solutions rsCase angebotenen Schnittstellen und Module in rsCase eingebunden werden. Zur Übernahme von TKÜ-Daten aus der TKÜ-Anlage wurde eine weitere Schnittstelle geschaffen.

d) Welche Datenbanken werden von rsCase, bCase oder anderen rola-Produkten abgefragt, wie es von rola als „Einmalerfassung – Mehrfachnutzung“ beworben wird?

Aus dem Fallbearbeitungssystem b-case heraus kann eine Abfrage an die in Inpol-Fall geführten Verbunddateien über die BLOS-Schnittstelle erfolgen. Auf welche Verbunddatei durch welchen Anwender zugegriffen werden darf, wird im Einzelfall über das in Inpol-Fall und b-case integrierte Rechte- und Rollenkonzept festgelegt.

---

[22] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

e) Welche Verfahren einer „automatischen Datenübernahme“ kommen hierbei zur Anwendung?

Eine „automatische Datenübernahme“ erfolgt bei Abfragen von Verbunddateien in Inpol-Fall über die BLOS-Schnittstelle nicht.

f) Wie ist die Nutzung der „Antiterrordatenbank“ oder von Inpol technisch und rechtlich geregelt?

Die rechtlichen Regelungen zu Inpol finden sich im BKAG, die zur Antiterrordatei im Antiterrordateigesetz. Die Details bezüglich der einzelnen Dateien sind in den jeweiligen Errichtungsanordnungen beschrieben. Technisch wird durch ein umfangreiches Berechtigungsverfahren und sonstige technische Vorkehrungen sichergestellt, dass die in den Errichtungsanordnungen niedergelegten Zugriffsregelungen eingehalten werden.

g) Inwieweit können kriminaltechnische Spuren eingebunden werden, und welche weiteren Anwendungen existieren hierzu?

In b-case können derzeit keine kriminaltechnischen Spuren erfasst werden. Für kriminaltechnische Vorgänge existieren die Vorgangsbearbeitungssysteme KISS und FISH, in denen auch kriminaltechnischen Spuren eingebunden werden können.

h) Inwieweit kann die genutzte rola-Software über eine Personenrecherche auch biometrische Daten verarbeiten?

Ein Abgleich biometrischer Daten ist im FBS b-case nicht vorgesehen.

i) Welche Module existieren zur Erhebung und Einbindung von Geodaten?

Das Fallbearbeitungssystem b-case verfügt über das Modul „GIS-Schnittstelle“, welches den Zugriff von b-case auf einen zentralen Karten-Server und die Visualisierung von geografischen Informationen innerhalb von b-case ermöglicht. Grundsätzlich können Geodaten auch manuell erfasst oder von der TKÜ-Anlage an b-case übergeben werden. Über Module zur Erhebung und Einbindung von Geodaten verfügt b-case nicht.

j) Haben das BKA oder andere Bundesbehörden jemals vom Data Mining- und Statistik-Modul von der rola-Software Gebrauch gemacht?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[23]

k) Inwieweit kann die beim BKA genutzte rola-Software für Maßnahmen in Echtzeit genutzt werden?

Das Fallbearbeitungssystem b-case verfügt über keine „Echtzeit-Funktionalitäten“.

l) Wie ist es technisch umgesetzt, dass für neu eingegangene Informationen eine Meldung ausgegeben werden kann?

Das Fallbearbeitungssystem b-case verfügt über ein Ereignismeldesystem für Systemnachrichten, Meldungen und Mails.

---

[23] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

m) Wie ist das Berechtigungskonzept innerhalb von rsCase bzw. ähnlicher Anwendungen geregelt, und wer trifft im Ermittlungsfall die jeweiligen Bestimmungen hierzu?

Inhalt, Art der Daten, Anlieferung und Zugriffsbefugnisse für einzelne Dateien sind in der jeweiligen dateispezifischen Errichtungsanordnung geregelt, die auf die jeweilige Rechtsgrundlage verweist. Über eine Berechtigungsverwaltung wird sichergestellt, dass die in den Errichtungsanordnungen fixierten Regelungen eingehalten werden. Die Berechtigung der Sachbearbeiter im Ermittlungsverfahren wird von der Berechtigungsverwaltung auf Antrag der ermittlungsführenden Abteilung eingerichtet.

20. Wie wurde die Vergabe und Beschaffung von rola-Software in den letzten zehn Jahren geregelt?

a) In welchen Fällen wurde rola-Software ohne Vergabebekanntmachung beschafft, und wie wurde das Verfahren im Einzelnen begründet?

BKA

Die Vergabe und Beschaffung von rola-Software unterliegt den allgemeinen beschaffungsrechtlichen Rahmenbedingungen. Der Auftrag zur Lieferung eines „Ermittlungs- und Auswertesystems“ der Firma rola Security Solutions GmbH an das BKA erfolgte im November 2006 nach vorheriger Marktsichtung im Zuge einer Freihändigen Vergabe ohne Teilnahmewettbewerb gemäß § 3 Nummer 1 Absatz 4 und Nummer 4 Buchstabe a und g der Verdingungsordnung für Leistungen – Teil A in der Fassung vom 6. April 2006. Der Vertrag wurde mit einer Laufzeit von fünf Jahren geschlossen.

BfV

In zwei Fällen wurde im BfV nach vorheriger Marktsichtung und Prüfung alternativer Produkte in freihändiger Vergabe Software der Firma rola Security Solution GmbH beschafft. Gerechtfertigt war dieses Vorgehen gemäß VOL/A unter anderem auch wegen der Notwendigkeit zur Geheimhaltung.

BPOL

Antwort analog BKA, der Vertrag wurde gemeinsam für BKA und BPOL geschlossen (Synergieeffekte bei der Beschaffung). Die Vergabe und Beschaffung von rola-Software unterliegt den vorgegebenen beschaffungsrechtlichen Rahmenbedingungen. Der Bundespolizei sind keine Fälle bekannt, in denen eine gesetzlich geforderte Vergabebekanntmachung nicht durchgeführt wurde.

ZFD

Bei diversen Landespolizeien wird die Software rsCase (oder eine Variante, z. B. Easy) der Firma Rola genutzt. Im Rahmen der Zusammenarbeit in Gemeinsamen Ermittlungsgruppen Rauschgift (GER) bedienen fallweise auch Beschäftigte des ZFD die auf den Systemen der betreffenden Landespolizei installierten Werkzeuge. Ein Erwerb von Software-Lizenzen durch das ZKA war erforderlich, damit ZFD-Bedienstete in den GERen weiterhin auf das Softwareprodukt zugreifen können. Der Erwerb erfolgte in diesem Fall im Rahmen der freihändigen Vergabe an den einzigen in Betracht kommenden Bieter. Die zwingende Notwendigkeit der produktbezogenen Beschaffung ergab sich aus Kompatibilitätserfordernissen wie z. B. der erforderlichen gemeinsamen Nutzung. Das entsprechende Produkt konnte aufgrund von zwingenden Vorgaben des Herstellers nur über lizenzierte Handelspartner mit Gebietsschutz bezogen werden. Dies galt auch für die diesbezüglichen Pflegeleistungen.

b) Welche Kosten entstehen für den technischen Betrieb, Wartung und Pflege von rola-Software, und wer führt diese aus?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[24]

c) Welche Kosten sind im Einzelfall für die Beschaffung von Zusatzmodulen entstanden?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[25]

d) Welche weiteren laufenden Kosten fallen an?

BKA

b-case wird – wie alle anderen polizeilichen Informationssysteme – im BKA auf einer technischen Standardplattform betrieben, welche die Server, Datenbanken und Sicherheitsmechanismen bereitstellt. Für diese Plattform fallen die für den Betrieb üblichen Lizenz- sowie Wartungs- und Pflegekosten an.

BPOL

Zusätzliche Kosten können durch Umsetzung von neuen fachlichen Anforderungen etc. entstehen. b-case wird – wie alle anderen polizeilichen Informationssysteme – bei der BPOL auf einer technischen Standardplattform betrieben, welche die Server, Datenbanken und Sicherheitsmechanismen bereitstellt. Für diese Plattform fallen die für den Betrieb üblichen Lizenz- sowie Wartungs- und Pflegekosten an.

ZFD

Weitere laufende Kosten im ZFD fallen nicht an, da die Software auf den Rechnern der jeweiligen Landespolizei betrieben wird.

BfV

Die eingesetzte rola-Software wird im BfV auf einer technischen Standardplattform betrieben, welche Server, Datenbanken und Sicherheitsmechanismen bereitstellt. Für diese Plattform fallen die für den Betrieb üblichen Lizenz- sowie Wartungs- und Pflegekosten an.

Darüber hinaus fallen derzeit keine weiteren laufenden Kosten durch die Firma rola Security Solution GmbH an.

e) Welche Errichtungsanordnungen existieren zu den einzelnen rola-Anwendungen?

BKA

In der Abteilung ST des BKA existieren folgende Errichtungsanordnungen zu den rola-Anwendungen (b-case Dateien):

– EGE Ausland-S

– EGE Ausland-Z

– IntTE-Gefahrenabwehrsachverhalte

[24, 25] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

– IntTE-Gefahrenermittlungssachverhalte
– IntTE-S
– IntTE-Z
– PMK-Finanz-Z
– PMK-links-S
– PMK-links-Z
– PMK-rechts-S
– PMK-rechts-Z
– Spionage/Tec-S
– Spionage-Tec-Z.

In der als Anlage unmittelbar beigefügten Übersicht sind alle aktuell in der Abteilung SO geführten Dateien aufgelistet, sofern sie auf der Basis der Produkte b-case oder Analyst's Notebook betrieben werden. Für jede der genannten Dateien existiert eine Errichtungsanordnung. Soweit es sich bei einem Eintrag in der Liste um eine ermittlungsbegleitende Datei handelt, wurde der Dateiname aus Sicherheitsgründen nicht angegeben.

BPOL

Für das Fallbearbeitungssystem der Bundespolizei existiert eine gültige Errichtungsanordnung.

BfV

Die bisher für das Vorgängersystem existierenden Errichtungsanordnungen werden derzeit überarbeitet und vor Inbetriebnahme von NADIS WN in Kraft gesetzt. Für die Analyse von Daten aus der TKÜ (Telekommunikationsverkehrsdaten) im Bereich der PG „Neue Analyse Methoden" (PG NAM) existiert eine „Dateianordnung des BfV zur Auswertung von Telekommunikationsverkehrsdaten (TKVD-Datei)".

ZFD

Da die rola-Anwendung „rs-case" lediglich auf Hardware der Polizei installiert ist und nur dort zum Einsatz kommt, existiert hierfür im ZFD keine Errichtungsanordnung.

21. Seit wann gilt rsCase als „bundesweit abgestimmtes Kerndatenmodell" unter den Ländern (Sächsischer Landtag, Drucksache 5/6190)?

Seit 2008 gibt es ein in der Interessengemeinschaft Fall und Analyse (IGFA) abgestimmtes Kerndatenmodell. Das Kerndatenmodell definiert, welche Daten bei einem Kerndatenexport und -import aus rsCase mindestens enthalten sein müssen.

a) In welchen länderübergreifenden Arbeitsgruppen wird die Nutzung von rola-Software durch Polizeibehörden begleitet oder ausgewertet?

Im Rahmen der Interessengemeinschaft Fall und Analyse (IGFA) wird u. a. auch die Nutzung und Weiterentwicklung von rsCase thematisiert. Die IGFA ist ein Mittel der Zusammenarbeit der Produktverantwortlichen der polizeilichen Fallbearbeitungssysteme.

b) Trifft es zu, dass das BKA in seiner Rolle als Zentralstelle den Ländern für bund-/länderübergreifende gemeinsame Ermittlungen, z. B. im Staatsschutz, den Einsatz von rsCase bzw. bCase empfiehlt oder sogar für den Datentausch vorgibt?

Nein. Das BKA spricht in seiner Rolle als Zentralstelle für länderübergreifende gemeinsame Ermittlungen weder Empfehlungen zur Nutzung einer bestimmten Software aus, noch gibt das BKA bei länderübergreifenden gemeinsamen Ermittlungen die Nutzung von rsCase für den Datentausch vor.

c) Falls ja, aufgrund welcher technischer und wirtschaftlicher Erwägungen wird rola-Software gegenüber anderen Produkten bevorzugt?

Es wird auf die Antwort zu Frage 21b verwiesen.

d) Trifft es zu, dass das beim BKA eingesetzte bCase keine Informationen an Inpol-Fall weitergeben kann, und falls ja, welcher einmalige und laufende Aufwand entsteht dem BKA durch eine etwaige Mehrfacherfassung von Daten in beiden Systemen?

Nein, das Fallbearbeitungssystem b-case verfügt über die BLDS zu Inpol-Fall.

22. Seit wann nutzt das BKA das Violent Crime Linkage Analysis System (ViCLAS), und wie wurde die Beschaffung geregelt?

Die Datenbank „ViCLAS“ ist seit dem Jahr 2000 aufgrund eines Beschlusses der AG Kripo im Wirkbetrieb. Die Software für die Datenbank wurde zunächst kostenfrei der deutschen Polizei von der kanadischen Royal Canadian Mounted Police (RCMP) zur Nutzung überlassen. Seit 2006 fallen jährliche Lizenzgebühren in Höhe von 30 000 Euro an, die vom BKA übernommen werden.

a) Mit welcher Zweckbestimmung wurde das System errichtet?

Laut Errichtungsanordnung vom 30. September 2008 dient die Datei folgenden Zwecken:

– Erkennung von Tatzusammenhängen bei Gewaltdelikten
– Täteridentifizierung und Zusammenführung von Serien im Bereich der sexuellen Gewaltdelikte und der Tötungsdelikte
– Gewinnung von Präventionsansätzen
– Beobachtung der Kriminalitätsentwicklung in den relevanten Delikts- und Tatfeldern.

b) Auf welche Datenbestände greift ViCLAS im Einzel- und im Regelfall zu?

Es gibt keine Schnittstelle zu anderen polizeilichen Informationssammlungen/Datenbeständen.

c) Welche Kriminalitätsphänomene werden mit ViCLAS untersucht?

In der Datei werden Informationen über versuchte oder vollendete Straftaten in den folgenden Deliktsfeldern gespeichert:

– Straftaten gegen das Leben
– Straftaten gegen die sexuelle Selbstbestimmung unter Anwendung oder Androhung von Gewalt

– Vermisstenfälle, bei denen die Gesamtumstände auf ein Verbrechen hindeuten
– Verdächtiges Ansprechen von Kindern und Jugendlichen, wenn ein sexuelles Gewaltmotiv vermutet werden kann und nach Sachlage tatsächliche Anhaltspunkte für eine geplante schwerwiegende Straftat vorliegen
– Persönlich motivierte Straftaten mit familiärer oder partnerschaftlicher Vorbeziehung (nur bei Vorliegen besonderer Tatumstände).

d) Hat ViCLAS Zusammenhänge zwischen einzelnen Verbrechen erkannt, und wenn ja, zwischen wie vielen in den letzten fünf Jahren?

Die Datenbank ViCLAS erkennt keine Zusammenhänge zwischen Verbrechen. Sie ist ein Hilfsmittel für besonders geschulte polizeiliche Fallanalytiker. Diese können mit Hilfe der Datenbank mögliche Tatzusammenhänge erkennen und begründen diese Tatzusammenhangsvermutungen in Form eines Analyseberichts. Die Ergebnisse dieser mit Hilfe der Datenbank erarbeiteten potenziellen Tatzusammenhänge haben die Qualität eines Ermittlungshinweises für die beteiligten sachbearbeitenden Dienststellen.

Im Zeitraum vom 19. Februar 2004 bis zum 26. Mai 2010 wurden von den deutschen Fachdienststellen für Operative Fallanalyse insgesamt 619 potenzielle Tatzusammenhänge mit Hilfe von ViCLAS erarbeitet. Davon konnte in 211 Fällen die Tatzusammenhangsvermutung durch die ermittelnden Dienststellen bestätigt werden.

e) Wurde auch die Mordserie, die vom „Nationalsozialistischen Untergrund“ verantwortet wird, mit ViCLAS analysiert?

Die Tötungsdelikte mit der Tatwaffe Ceska, die zwischenzeitlich dem „Nationalsozialistischen Untergrund“ zugeordnet werden, waren als ungeklärte Tötungsdelikte mit unklarer Motivlage u. a. in ViCLAS erfasst. Die durch kriminaltechnische Gutachten bekannten Tatzusammenhänge waren ebenfalls erfasst. Entsprechende Analysen wurden von der Fachdienststelle für Operative Fallanalysen beim PP München durchgeführt. Die ViCLAS-Recherchen führten nicht zur Erkennung neuer möglicher Fallzusammenhänge. Auch der Polizistenmord in Heilbronn in 2007 wurde in ViCLAS erfasst. Die Recherche durch die Fachdienststelle für Operative Fallanalysen beim LKA Baden-Württemberg führte nicht zur Erkennung neuer möglicher Fallzusammenhänge.

f) Sofern ViCLAS Zusammenhänge findet, wie wird dann innerhalb des BKA weiter verfahren?

Die Erarbeitung von Tatzusammenhängen mit Hilfe der ViCLAS-Datenbank findet in der Regel nicht im BKA sondern bei den Fachdienststellen für Operative Fallanalyse der Länder statt. Wenn eine Fachdienststelle für Operative Fallanalyse mit Hilfe von ViCLAS einen fallanalytisch begründeten Tatzusammenhangsverdacht erarbeiten kann, werden die Inhalte in einem Analysebericht schriftlich fixiert und den für die Fälle zuständigen Ermittlungsdienststellen mitgeteilt. Begleitend zur Mitteilung dieser Ermittlungshinweise werden in geeigneten Fällen Beratungsleistungen im Hinblick auf die anzustellenden Ermittlungshandlungen angeboten. Als zusätzliche Maßnahme kann die zuständige Fachdienststelle für Operative Fallanalyse in geeigneten Fälle eine vergleichende Fallanalyse durchführen, die eine intensivere Befassung mit den Einzelfällen und eine umfassende vergleichende Bewertung beinhaltet, als sie bei der ViCLAS-Sachbearbeitung üblich ist.

23. In welcher Form soll die Zusammenarbeit zwischen Landes- und Bundesbehörden sowie weiteren Akteuren innerhalb des „Kompetenzzentrums Informationstechnische Überwachung“ (ITÜ) erfolgen?

Die Zusammenarbeitsformen zwischen Landes- und Bundesbehörden sowie weiteren Akteuren innerhalb des „Kompetenzzentrums Informationstechnische Überwachung“ (CC ITÜ) werden derzeit im Rahmen des hierfür im BKA eingesetzten Aufbaustabes untersucht.

a) In welcher Höhe soll das ITÜ im Jahr 2012 mit Finanzmitteln ausgestattet werden?

Für Aufgaben des CC ITÜ wurden im Bundeshaushalt 2012 2,2 Mio. Euro veranschlagt.

b) In welcher Höhe sind finanzielle Mittel für die Programmierung von Computerspionageprogrammen (staatliche Trojaner) vorgesehen?

Vom CC ITÜ wird ausschließlich Software für die informationstechnische Überwachung unter den bestehenden rechtlichen Voraussetzungen entwickelt. Die konkrete Verteilung der finanziellen Mittel für die Aufgaben des CC ITÜ ist Gegenstand der derzeitigen Aufbaukonzeption. Insofern sind die Aufwendungen für Programmierleistungen im Einzelnen nicht zu beziffern.

c) Welche Akteure (Ämter, Behörden, Institute, Firmen, Stiftungen etc.) werden in deren Entwicklung eingebunden?

Auf die Antwort zu Frage 23 wird verwiesen.

d) Wie ist eine Kontrolle des Kompetenzzentrums bislang vorgesehen?

Im Rahmen der üblichen Kontrollfunktionen unterliegt das CC ITÜ der Fachaufsicht des BMI. Weitergehende Kontrollfunktionen, wie z. B. durch das einzurichtende Expertengremium, werden derzeit konzipiert.

e) Auf welche Art und Weise sollen von Bundesbehörden Programme zur Quellen-TKÜ zukünftig auf dem Zielsystem installiert werden, und auf welche Art und Weise geschah dies bislang?

Die Installation von Programmen zur Quellen-TKÜ erfolgt grundsätzlich analog zu der Installation sonstiger Programme. Im Unterschied zu der Installation sonstiger Programme durch den Berechtigten besitzt die Stelle, welche die Quellen-TKÜ-Software installiert, in der Regel jedoch nicht den benötigten direkten Zugriff auf das Zielsystem.

Sofern kein direkter Zugriff auf das Zielsystem gegeben ist, gibt es verschiedene Formen, Programme zur Quellen-TKÜ zu installieren. Diese werden im jeweiligen Einzelfall basierend auf einer vorangehenden Analyse des Zielsystems ausgewählt.

24. Über welche technischen Funktionalitäten, insbesondere zur Erkennung von Gesichtern, verfügt die von Bundesbehörden laut der Antwort auf die Schriftliche Frage 15 auf Bundestagsdrucksache 17/8102 genutzte Software?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[26]

a) In wie vielen Fällen wurde bereits Software der Firma Cognitech oder anderer Hersteller genutzt, um Lichtbilder mit der Inpol-Datenbank abzugleichen bzw. sofern hierfür keine Statistik existiert, in welcher Größenordnung bewegt sich die Praxis?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[27]

b) Wie hoch ist die Trefferquote derart abgefragter Identifizierung?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[28]

c) Mit welchen forensischen Anwendungen welcher Hersteller arbeiten Bundesbehörden bezüglich der Rekonstruktion unkenntlich gemachter Gesichter?

Kriminaltechnische Rekonstruktionen unkenntlich gemachter Gesichter werden im BKA bisher ohne spezielle Software durchgeführt.

Die Bundespolizei und die Behörden der Zollverwaltung nutzen solche forensischen Anwendungen nicht.

25. Mit welcher Technologie sind die 52 Beweissicherungs- und Dokumentationskraftwagen (BeDoKw) ausgestattet, die von den Firmen Gero, Elettronica und Vidit Systems gefertigt wurden und deutschen Bereitschaftspolizeien der Länder in Anwesenheit der Bundespolizei und des Beschaffungsamtes des Bundesministeriums des Innern überreicht wurden?

a) Wie ist die Bundesregierung in die Organisation und Durchführung der Beschaffung eingebunden?

Eine Bund-Länder-Projektgruppe unter Leitung der Bundespolizei hat die technisch-betriebliche Bedarfsbeschreibung erstellt und die Leistungsbeschreibung mit dem Beschaffungsamt des Bundesministeriums des Innern abgestimmt. Die Beschaffungsmaßnahme im engeren Sinne, welche auf Grundlage der durch die Projektgruppe erarbeiteten Bedarfsbeschreibung für die BeDoKw erfolgte, wurde durch das Beschaffungsamt des Bundesministeriums des Innern realisiert.

b) Welche Produkte der Firmen Vidit, Geroh und Elettronica wurden verbaut?

c) Welche „Elektro- und IuK-Ausstattung“ (ausschreibungen.dgmarket.com/tenders/np-notice.do~5840668) anderer Hersteller wurden ausgeliefert, um Lageinformationen „visuell und akustisch aufzuzeichnen, zu selektieren, zu analysieren und bei Bedarf an übergeordnete Stellen zu übermitteln“ (tinyurl.com/c6uthg2)?

[26, 27, 28] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

d) Mittels welcher Verfahren werden „alle gesammelten Daten“ im Fahrzeug verarbeitet und übermittelt?

e) Welche weiteren „Fähigkeiten“ können angesichts des „modularen Aufbaus“ integriert werden, und welche Überlegungen wurden hierfür angestellt?

f) Welche andere Firma hatte sich außer Elettronica um die Fertigung der Fahrzeuge beworben, und wieso wurde Elettronica bevorzugt?

Siehe hierzu die Ausführungen in der Anlage, die in der Geheimschutzstelle des Deutschen Bundestages hinterlegt ist.[29]

[29] Das Bundesministerium des Innern hat die Antwort als „VS – geheim“ eingestuft.
Die Antwort ist in der Geheimschutzstelle des Deutschen Bundestages hinterlegt und kann dort nach Maßgabe der Geheimschutzordnung eingesehen werden.

Anlage zu Frage 20e

Lfd. Nummer	Dateiname	Zweck/Delikt	Dateityp	Anordnungsdatum
1	3hoch2	Auswerteprojekt bez. Computerkriminalität	Auswertedatei	09.05.2009
2		Verdacht des Fälschens und Ausspähens von Daten	Amtsdatei	11.02.2009
3		Verdacht der Beihilfe zum Mord	Amtsdatei	11.08.2008
4		Verdacht des Verstoßes gegen das Arzneimittelgesetz	Amtsdatei	09.04.2009
5		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	19.12.2008
6		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	04.05.2009
7		Verdacht der Hehlerei, der Geldwäsche und der Erpressung	Amtsdatei	27.04.2009
8		Verdacht der Verbreitung von Kinderpornografie im Internet	Amtsdatei	17.01.2007
9		Verdacht des Ausspähens von Daten und der Computersabotage	Amtsdatei	13.02.2009
10		Verdacht der Geldwäsche	Verbunddatei	31.10.2005
11		Verdacht der Fälschung von Zahlungskarten mit Garantiefunktion	Amtsdatei	26.03.2009
12		Verdacht des Bandendiebstahls und der gewerbsmäßigen Hehlerei	Amtsdatei	23.07.2009
13		Verdacht der Manipulation von Geldautomaten und des Ausspähens von Zahlungskartendaten	Amtsdatei	28.04.2009
14		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	19.12.2008
15		Verdacht der Verbreitung, des Erwerbs und des Besitzes von kinderpornografischen Schriften	Amtsdatei	20.05.2009
16		Verdacht der Geldwäsche	Verbunddatei	23.07.2009
17		Verdacht der Geldwäsche	Verbunddatei	22.01.2007
18	Eigentum	Clusterdatei Eigentumskriminalität	Zentraldatei	17.01.2008
19		Ermittlungsverfahren wegen Eigentumsdelikten	Amtsdatei	30.09.2009
20		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	22.02.2008
21		Ermittlungsverfahren wegen Fälschungsdelikten	Amtsdatei	30.09.2009
22		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	06.04.2009
23	FK (Fälschungskriminalität)	Clusterdatei Fälschungskriminalität	Zentraldatei	27.08.2009
24		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	29.04.2008
25		Verdacht der Verbreitung von kinderpornografischen Schriften und des schweren sexuellen Missbrauchs von Kindern	Amtsdatei	08.01.2009
26		Ermittlungsverfahren wegen Verdachts der Geldwäsche	Amtsdatei	30.09.2009
27		Verdacht der Erpressung und des Ausspähens von Daten	Amtsdatei	16.02.2009

Lfd. Nummer	Dateiname	Zweck/Delikt	Dateityp	Anordnungsdatum
28		Verdacht der Geldwäsche	Verbunddatei	03.11.2008
29	GS (Gewalt- und Schwer-kriminalität)	Clusterdatei Gewalt- und Schwerkriminalität	Zentraldatei	22.01.2009
30		Ermittlungsverfahren wegen Delikten der Gewalt- und Schwer-kriminalität	Amtsdatei	30.09.2009
31	GW (Geldwäsche)	Clusterdatei Geldwäsche	Zentraldatei	27.08.2009
32		Verdacht des Computerbetruges	Amtsdatei	18.02.2009
33		Verdacht der Untreue und des Verstoßes gegen das Wertpapier-handelsgesetz	Amtsdatei	15.01.2008
34	IUK (Informations- u Kommunikationskriminalität)	Clusterdatei Informations- und Kommunikationskriminalität	Zentraldatei	27.08.2009
35		Ermittlungsverfahren wegen IuK-Delikten	Amtsdatei	30.09.2009
36		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	27.05.2009
37		Verdacht des Verstoßes gegen das Wertpapierhandelsgesetz	Amtsdatei	16.05.2008
38		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	23.12.2008
39		Verdacht des schweren Menschenhandels und des Missbrauchs von Jugendlichen	Amtsdatei	05.11.2008
40		Verdacht der Geldwäsche	Amtsdatei	03.04.2008
41		Verdacht des gewerbsmäßigen Einschleusens von Ausländern	Amtsdatei	30.01.2009
42		Verdacht der Geldwäsche	Verbunddatei	19.06.2009
43		Verdacht der Geldwäsche	Amtsdatei	02.07.2009
44		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	09.05.2008
45	OK (Organisierte Kriminalität)	Clusterdatei Organisierte Kriminalität	Zentraldatei	27.08.2009
46		Verdacht des Menschenhandels zur sexuellen Ausbeutung	Amtsdatei	26.01.2009
47		Verdacht des Verstoßes gegen das Betäubungsmittelgesetz	Amtsdatei	15.07.2009
48		Verdacht des Verstoßes gegen das Arzneimittelgesetz	Amtsdatei	17.04.2009
49		Verdacht des Betruges pp. im Zusammenhang mit der Anwendung von Doping-Mitteln	Amtsdatei	08.11.2006
50		Verdacht der Verbreitung von kinderpornografischen Schriften	Amtsdatei	09.09.2008
51		Ermittlungsverfahren wegen Verstoßes gegen das Betäubungs-mittelgesetz	Amtsdatei	30.09.2009

Lfd. Nummer	Dateiname	Zweck/Delikt	Dateityp	Anordnungsdatum
52	RG (Rauschgiftkriminalität)	Clusterdatei Rauschgiftkriminalität	Zentraldatei	27.08.2009
53		Verdacht des gewerbsmäßigen Inverkehrbringens von Arzneimitteln zu Dopingzwecken	Amtsdatei	05.03.2008
54	Sichel	Auswertung der Rauschgiftkriminalität im Bereich Zentralasen/ Südwestasien und entlang der Balkan-Seidenstraße	Amtsdatei	21.11.2005
55		Verdacht des Verstoßes gegen das WaffG	Amtsdatei	24.11.2008
56		Verdacht der Untreue	Amtsdatei	08.02.2008
57		Verdacht der Geldwäsche	Verbunddatei	09.11.2010
58		Verdacht der Geldwäsche und Verstoßes gegen das Betäubungs-mittelgesetz	Verbunddatei	13.01.2011
59		Verdacht der Geldwäsche	Amtsdatei	06.08.2009
60		Ermittlungsverfahren wegen Fälschung- u. Betrugsdelikten u. a.	Amtsdatei	31.07.2009
61		Verdacht des Menschenhandels	Amtsdatei	11.08.2009
62		Verdacht der Geldwäsche	Verbunddatei	17.03.2008
63		Verdacht des Betruges im Zusammenhang mit der Anwendung von Dopingmitteln	Amtsdatei	02.07.2007
64		Verdacht des Betruges im Zusammenhang mit der Anwendung von Dopingmitteln	Amtsdatei	07.07.2008
65		Verdacht des Verstoßes gegen das Waffengesetz, Betruges und der Urkundenfälschung	Amtsdatei	16.06.2008
66		Verdacht des schweren sexuellen Missbrauchs	Amtsdatei	09.09.2008
67		Verdacht der Bildung einer kriminellen Vereinigung	Amtsdatei	11.08.2008
68		Verdacht der Geldwäsche	Amtsdatei	16.07.2009
69		Ermittlungsverfahren wegen Wirtschaftskriminalität, Korruptions-straftaten und Umwelt- und Verbraucherschutzdelikten	Amtsdatei	30.09.2009
70		Verdacht der Geldwäsche	Verbunddatei	30.06.2008

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333