

Beschlussempfehlung und Bericht des Innenausschusses (4. Ausschuss)

1. zu dem Gesetzentwurf der Fraktionen der CDU/CSU und SPD – Drucksache 16/9588 –

**Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen
Terrorismus durch das Bundeskriminalamt**

2. zu dem Gesetzentwurf der Bundesregierung – Drucksache 16/10121 –

**Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen
Terrorismus durch das Bundeskriminalamt**

A. Problem

Ziel des Gesetzentwurfs ist die Verbesserung der Möglichkeiten bei der Bekämpfung des internationalen Terrorismus durch das Bundeskriminalamt (BKA).

B. Lösung

Zu den Nummern 1 und 2

Das Bundeskriminalamt erhält in bestimmten Fallgruppen die Aufgabe der Abwehr von Gefahren des internationalen Terrorismus sowie entsprechende Befugnisse.

Annahme der Gesetzentwürfe in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

C. Alternativen

Ablehnung der Gesetzentwürfe.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugaufwand

Keine

2. Vollzugsaufwand

Die Wahrnehmung der neuen Aufgaben des BKA erfordert 130 Planstellen/Stellen und im ersten Jahr nach Inkrafttreten einen im Wesentlichen durch einmalige Aufwendungen bedingten Finanzaufwand in Höhe von rund 18,5 Mio. Euro. In den Folgejahren fallen laufende Kosten (Sach- und Personalkosten) in Höhe von jährlich etwa 10,2 Mio. Euro an.

Sofern die Wahrnehmung der neuen Aufgaben aus dem Bundeskriminalamtgesetz (BKAG) auch zu tatsächlichen Haushaltsmehrbelastungen führt, wird darüber im Rahmen der Aufstellung des Haushalts zum Einzelplan 06 entschieden.

E. Sonstige Kosten

Auswirkungen auf Einzelpreise und das Preisniveau, insbesondere das Verbraucherpreisniveau, sind nicht zu erwarten.

F. Bürokratiekosten

Es entstehen für die Wirtschaft, die Bürgerinnen und Bürger und die Verwaltung neue Bürokratiekosten.

1. Bürokratiekosten der Wirtschaft

Es werden vier neue Informationspflichten eingeführt. Die durch den Aufwand für die Erfüllung dieser Pflichten entstehenden Bürokratiekosten sind – auch im Rahmen einer Schätzung – nicht bezifferbar.

2. Bürokratiekosten der Bürgerinnen und Bürger

Es werden zwei neue Informationspflichten eingeführt. Durch den Aufwand für die Erfüllung dieser Pflichten entstehen Bürokratiekosten.

3. Bürokratiekosten der Verwaltung

Es werden 26 neue Informationspflichten eingeführt. Durch den Aufwand für die Erfüllung dieser Pflichten entstehen Bürokratiekosten.

Diese Bürokratiekosten sind im Interesse einer effektiven Gefahrenabwehr nicht vermeidbar und geboten. Weniger belastende Alternativen zu den Informationspflichten bestehen nicht.

Beschlussempfehlung

Der Bundestag wolle beschließen,

die Gesetzentwürfe auf Drucksachen 16/9588 und 16/10121 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 Nr. 5 wird wie folgt geändert:

a) In § 20c Abs. 3 wird nach Satz 2 folgender Satz eingefügt:

„Eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder Nr. 4 der Strafprozessordnung genannte Person ist auch in den Fällen des Satzes 2 zur Verweigerung der Auskunft berechtigt.“

b) In § 20j Abs. 4 werden die Sätze 2 bis 4 aufgehoben.

c) § 20k wird wie folgt geändert:

aa) Absatz 2 Satz 2 und 3 wird wie folgt gefasst:

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

bb) Absatz 7 wird wie folgt geändert:

aaa) Satz 3 wird wie folgt gefasst:

„Erhobene Daten sind unverzüglich vom Datenschutzbeauftragten des Bundeskriminalamtes und zwei weiteren Bediensteten des Bundeskriminalamtes, von denen einer die Befähigung zum Richteramt hat, auf kernbereichsrelevante Inhalte durchzusehen.“

bbb) Nach Satz 3 wird folgender neue Satz 4 eingefügt:

„Der Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Abs. 3 BDSG).“

ccc) Der neue Satz 6 wird wie folgt gefasst:

„Besteht zwischen den Beteiligten Uneinigkeit, ob Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, oder hat einer der Beteiligten Zweifel darüber, sind die Daten, sofern sie nicht gelöscht werden, unverzüglich dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung vorzulegen.“

d) § 20t Abs. 1 Satz 1 Nr. 1 wird wie folgt geändert:

Nach den Wörtern „oder nach“ wird die Angabe „§ 20n“ durch die Angabe „§ 20p“ ersetzt.

e) § 20v Abs. 5 wird wie folgt gefasst:

„(5) Das Bundeskriminalamt kann die nach diesem Unterabschnitt erhobenen personenbezogenen Daten an andere Polizeien des Bundes und der Länder sowie an sonstige öffentliche Stellen übermitteln, soweit dies erforderlich ist

1. zur Herbeiführung des gegenseitigen Benehmens nach § 4a Abs. 2 Satz 3,
2. zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit oder zur Verhütung von Straftaten, die in § 129a Abs. 1 und 2 des Strafgesetzbuches bezeichnet sind, im Falle einer Maßnahme nach den §§ 20h, 20k oder 20l nur zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit, insbesondere einer gemeinen Gefahr oder einer Lebensgefahr, oder

3. zur Verfolgung von Straftaten, wenn ein Auskunftsverlangen nach der Strafprozessordnung zulässig wäre. Daten, die nach den §§ 20h, 20k oder 20l erhoben worden sind, dürfen nur zur Verfolgung von Straftaten übermittelt werden, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht sind.

In den Fällen des Satzes 1 Nr. 2 ist § 20a Abs. 2 insoweit nicht anzuwenden, als die Gefahr im Zusammenhang mit Straftaten gemäß § 4a Abs. 1 Satz 2 stehen muss. Die vom Bundeskriminalamt nach diesem Unterabschnitt erlangten personenbezogenen Daten dürfen an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst übermittelt werden, wenn

1. tatsächliche Anhaltspunkte dafür bestehen, dass die Daten erforderlich sind zur Sammlung und Auswertung von Informationen über Bestrebungen in der Bundesrepublik Deutschland, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind, oder
2. bestimmte Tatsachen den Verdacht sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht begründen.

Die vom Bundeskriminalamt nach diesem Unterabschnitt erlangten personenbezogenen Daten dürfen an den Bundesnachrichtendienst übermittelt werden, wenn bestimmte Tatsachen den Verdacht begründen, dass diese Daten für die Erfüllung der Aufgaben des Bundesnachrichtendienstes nach § 1 Abs. 2 des Gesetzes über die den Bundesnachrichtendienst zur Sammlung von Informationen über die in § 5 Abs. 1 Satz 3 Nr. 1 bis 3 des Artikel 10-Gesetzes genannten Gefahrbereiche erforderlich sind. Nach § 20h erhobene Daten dürfen nur übermittelt werden, um bei dem Bundesamt für Verfassungsschutz, den Verfassungsschutzbehörden der Länder, dem Bundesnachrichtendienst oder dem Militärischen Abschirmdienst Auskünfte einzuholen, die für die Erfüllung der Aufgabe des Bundeskriminalamtes nach § 4a Abs. 1 Satz 1 erforderlich sind. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.“

2. Artikel 6 wird wie folgt gefasst:

„Artikel 1 §§ 4a, 20j und 20k ist fünf Jahre nach dem Inkrafttreten unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren.

3. Der bisherige Artikel 6 wird Artikel 7 und wie folgt gefasst:

„(1) Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

(2) Artikel 1 § 20k tritt am 31. Dezember 2020 außer Kraft.“

Berlin, den 10. November 2008

Der Innenausschuss

Sebastian Edathy
Vorsitzender

Helmut Brandt
Berichterstatter

Michael Hartmann (Wackernheim)
Berichterstatter

Frank Hofmann (Volkach)
Berichterstatter

Gisela Piltz
Berichterstatteerin

Ulla Jelpke
Berichterstatteerin

Wolfgang Wieland
Berichterstatter

Bericht der Abgeordneten Helmut Brandt, Michael Hartmann (Wackernheim), Frank Hofmann (Volkach), Gisela Piltz, Ulla Jelpke und Wolfgang Wieland

I. Zum Verfahren

1. Überweisung

Der Gesetzentwurf der Fraktionen der CDU/CSU und SPD auf **Drucksache 16/9588** wurde in der 170. Sitzung des Deutschen Bundestages am 20. Juni 2008 und der Gesetzentwurf der Bundesregierung auf **Drucksache 16/10121** wurde in der 179. Sitzung des Deutschen Bundestages am 25. September 2008 an den Innenausschuss federführend sowie an den Auswärtigen Ausschuss, den Rechtsausschuss und den Haushaltsausschuss gemäß § 96 GO-BT zur Mitberatung überwiesen.

2. Voten der mitberatenden Ausschüsse

Der **Auswärtige Ausschuss** hat in seiner 74. Sitzung am 5. November 2008 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 16/9588 und 16/10121 empfohlen.

Der **Rechtsausschuss** hat in seiner 116. Sitzung am 10. November 2008 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN empfohlen, den Gesetzentwurf in der Fassung des Änderungsantrags der Koalitionsfraktionen der CDU/CSU und SPD auf Ausschussdrucksache 16(4)505 anzunehmen.

Der **Haushaltsausschuss** wird seinen Bericht gemäß § 96 GO-BT gesondert abgeben.

3. Beratungen im federführenden Ausschuss

Der Innenausschuss hat in seiner 72. Sitzung am 25. Juni 2008 beschlossen, eine öffentliche Anhörung zu dem Gesetzentwurf durchzuführen. Die öffentliche Anhörung, an der sich elf Sachverständige beteiligt haben, hat der Innenausschuss in seiner 73. Sitzung am 15. September 2008 durchgeführt. Hinsichtlich des Ergebnisses der Anhörung wird auf das Protokoll der 73. Sitzung des Innenausschusses hingewiesen (Protokoll Nummer 16/73).

Der **Innenausschuss** hat in seiner 78. Sitzung am 10. November 2008 die Gesetzentwürfe auf Drucksachen 16/9588 und 16/10121 abschließend beraten. Als Ergebnis der Beratungen wurde empfohlen, die Gesetzentwürfe in der Fassung des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 16(4)505 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN anzunehmen.

Zuvor wurde der Änderungsantrag der Koalitionsfraktionen auf Ausschussdrucksache 16(4)505 mit demselben Stimenergebnis angenommen.

Zu den Konstellationen zum Bedarf der Normierung einer Eilfallregelung bei § 20k BKAG-E (Onlinedurchsuchung,

Online-DS, ODS) weisen die Koalitionsfraktionen auf folgende Beispielfälle, die den Beratungen zugrunde lagen und dem Protokoll der 78. Sitzung des Innenausschusses beige-fügt sind, hin:

In der Ausgangslage (Szenario) kann zum Bedarf der Eilfallregelung in § 20k BKAG-E analog den Erfahrungen im Sauerlandfall bei der Datenträgerauswertung („kryptierte Daten“) argumentiert werden: ZP legen auf der Festplatte kryptiert Daten ab. Selbst bei der Datenträgerauswertung nach Beschlagnahme können die Daten noch heute nicht ausgewertet werden.

Eine Onlinedurchsuchung wäre hier zielführend gewesen, die Konstellation einer Eilfallregelung kann seitens des BKA anhand des Szenarios bei Gefahr eines Anschlags auf ein U-Bahn-Netz einer Großstadt dargelegt werden.

Ausgangsfall

Beim BKA geht aus Großbritannien ein Hinweis auf Person X mit Wohnsitz in Deutschland ein, die dem britischen Geheimdienst wegen intensiver E-Mail-Kontakte zu einem in Geheimdienstkreisen einschlägig bekannten Islamisten Y aufgefallen ist. Mit dem Hinweis wird zugleich der Verdacht geäußert, dass Y einen Anschlag auf das U-Bahn-Netz einer noch nicht identifizierbaren europäischen Großstadt plane. Die Hinweise darauf erhielt Großbritannien durch einen V-Mann. Für einen Anfangsverdacht nach den §§ 129a, 129b StGB liegen bislang keine ausreichenden Hinweise vor.

Nach Erkenntnissen des britischen Geheimdienstes werden Kontakte ausschließlich per E-Mail unterhalten. Telefonische Absprachen finden nicht statt. Die E-Mails werden verschlüsselt versendet. Der britische Geheimdienst konnte daher nur die Tatsache solcher Kontaktaufnahmen und -pflege feststellen.

Y ist untergetaucht und demnach ist X der einzige Anknüpfungspunkt zur Verifizierung der Anschlagpläne und zur Abwehr der dadurch bestehenden Gefahr. Andere Maßnahmen wie z. B. eine offene Durchsuchung oder eine Wohnraumüberwachung kommen nicht in Betracht, da

- befürchtet wird, dass eine offene Maßnahme die Person Y und ggf. noch unbekannte weitere Beteiligte zu einer sofortigen Umsetzung der Anschlagpläne verleiten könnte,
- davon ausgegangen wird, dass vor dem Hintergrund des hochgradig konspirativen Verhaltens von X und Y (Versendung von ausschließlich verschlüsselten E-Mails) Unterlagen zu den Anschlagplänen auf dem Computersystem von X ebenfalls ausschließlich verschlüsselt abgespeichert sind (eine Beschlagnahme des Computersystems würde daher zu keinen Erkenntnissen führen).

Eine TKÜ-Maßnahme (TKÜ: Telekommunikationsüberwachung) ist alleine nicht zielführend. Da X nur kryptiert kommuniziert, läuft schon eine „konventionelle“ TKÜ ins Leere. Eine Quellen-TKÜ nach § 20I Abs. 2 BKAG-E ermöglicht dann in Einzelfällen zwar durch das eingesetzte Tool z. B.

bei VoIP/SKYPE die Ausleitung und Auswertung der ansonsten kryptierten Telekommunikation; die Inhalte anhängender kryptierter Dokumente erhält man aber über die Quellen-TKÜ nicht. Auf derartige Dokumente kann jedoch mit einer Onlinedurchsuchung dann zugegriffen werden, wenn sie von der Zielperson (ZP) geöffnet und gelesen oder bearbeitet werden.

Darstellung der Ermittlungsstufen im vorliegenden Fall

1. Konventionelle TKÜ: Feststellung, dass überhaupt nur kryptiert kommuniziert wird.
2. Quellen-TKÜ: Feststellung, dass auch die Dokumente/Anlagen der E-Mails verschlüsselt übermittelt werden, deren Verschlüsselung durch die Quellen-TKÜ nicht „geknackt“ wird.
3. Da die ZP die verschlüsselten E-Mails/Anlagen/Dokumente auf der Festplatte speichert, muss mit einer Online-DS auf diese Daten zugegriffen werden.

Daher kommt nur die Onlinedurchsuchung als Ultima Ratio zur Abwehr der Gefahr in Betracht. Es ist zu erwarten, dass mit dieser Maßnahme Dateien mit z. B. Bauplänen von U-Bahnnetzen europäischer Großstädte oder sonstige Hinweise auf Anschlagziel und -zeitpunkt sowie die geplante Vorgehensweise erlangt werden. Der konkrete Zeitpunkt des „Tages X“ für den geplanten Anschlag ist noch nicht abzusehen; auch wo der Anschlag begangen werden soll, ist den Ermittlern noch nicht bekannt.

1. Fallkonstellation

- Remote Forensic Software (RFS) wurde bei einer angeordneten und durchgeführten Onlinedurchsuchung eingesetzt.
- Maßnahme wurde beendet, da nicht ergiebig.
- RFS auf Zielsystem gelöscht.
- Später wird eine weitere Onlinedurchsuchung erforderlich.
- Geeignetes Tool (RFS) steht zur Verfügung.

Die RFS wurde bereits für eine zurückliegende Maßnahme des § 20k BKAG-E entwickelt und bei der Zielperson eingesetzt. Nach Beendigung der Maßnahme und Löschung der RFS auf dem Zielsystem ist aufgrund einer Lageänderung bzw. neuer Lageerkennnisse der Bedarf nach einer weiteren Onlinedurchsuchungsmaßnahme gegen die Zielperson erkannt worden. Eine kurzfristige Übermittlung bzw. Aufbringung des bereits bewährten Tools ist erneut notwendig, jedoch mit der Besonderheit, dass sich Vorbereitungsmaßnahmen wie die Erlangung von Kenntnissen über Lebensgewohnheiten der Zielperson bzw. von Kenntnissen über das Zielsystem usw. erübrigen. Die RFS ist damit sofort einsetzbar. Zeitverzug durch eine richterliche Anordnung (insbesondere an Wochenenden und in der Nachtzeit) könnte den Erfolg vereiteln, da zum einen terroristische Straftaten unbemerkt vorbereitet werden könnten und zum anderen in der Regel nur ein sehr kleines Zeitfenster für die Aufbringung der Remote Forensic Software auf den Zielrechner besteht.

Besonderheit in dieser Konstellation

- Erste Online-DS nach § 20k BKAG-E; umfangreiche Umfeldaufklärungen (DSL-Überwachung, Observation, VP-Informationen etc.) zum informationstechnischen System liegen vor, RFS wird einsatzfähig gemacht.
- Dauer der richterlichen Anordnung gem. § 20k BKAG-E: drei Monate. Maßnahme wird durchgeführt, entgegen der Erwartung aber nicht ergiebig. Wider Erwarten keine E-Mail-Kommunikation mittels ermittlungsrelevanter verschlüsselter Anlagen. Auf der Festplatte keine weiteren Ermittlungsansätze.
- Verlängerungsanordnung daher nicht geboten.
- Nach gesetzlicher Vorgabe wird das Tool gelöscht.
- Zweite Online-DS: Erst durch weitere Begleitmaßnahmen (auch: VP-Hinweis) wird bekannt, dass die ZP in der kommenden Nacht von einem Samstag auf einen Sonntag die wichtige Nachricht mittels verschlüsselter Dateianlage einer E-Mail erlangen wird (konkrete Anschlagsplanung!, Skizzen!; Anleitungen!).
- Das RFS-Tool ist hier bereits vorhanden, kann taktisch sofort eingesetzt werden, bis zum Montag (Erreichen eines Richters) darf nicht zugewartet werden.
- Eilfallregelung erforderlich.

2. Fallkonstellation

- RFS wurde bei einer angeordneten Onlinedurchsuchung vorbereitet.
- Maßnahme konnte jedoch aus taktischen Gründen nicht realisiert werden.
- Richterliche Anordnung läuft nach drei Monaten aus.
- Keine RFS auf dem Zielrechner.
- Später wird eine weitere Onlinedurchsuchung erforderlich und Realisierungsmöglichkeit (günstiges Zeitfenster) bietet sich.
- Auf das einsatzfähige Tool kann zurückgegriffen werden.

Eine vergleichbare Fallkonstellation besteht darin, dass in einem Fall eine richterliche Anordnung nach § 20k BKAG-E vorlag, durch Begleitmaßnahmen das RFS-Tool bezogen auf den Zielrechner fertiggestellt („einsatzfähig“) wurde, jedoch die Maßnahme faktisch nicht realisiert werden konnte (z. B.: Zielperson ging während des gesamten Zeitraums der befristeten Anordnung nicht „online“, so dass die RFS nicht aufgespielt werden konnte). Mit Ablauf der richterlichen Befristung endete die Anordnung, die Voraussetzungen einer Verlängerung lagen nicht vor. Durch andere polizeiliche Maßnahmen wird eine kurzfristige Lageänderung dahingehend festgestellt, dass die Zielperson nach längerer Zeit wieder das Zielsystem, ihren Rechner, für eine Internetverbindung nutzt. Hier kann der Bedarf einer Eilanordnung bestehen, da das Nutzungsverhalten der Zielperson nur eine kurze „Onlinezeit“ erwarten lässt und eine richterliche Entscheidung nicht zeitnah zu erlangen ist. Das RFS-Tool ist bereits einsatzfähig.

3. Fallkonstellation

- RFS wurde bei einer angeordneten Onlinedurchsuchung vorbereitet und
 - Maßnahme konnte aus taktischen Gründen nicht realisiert werden (siehe Fallkonstellation 2) oder
 - Maßnahme wurde durchgeführt (siehe Fallkonstellation 1).
- Maßnahme wurde beendet.
- Richterlicher Anordnungszeitraum läuft ab, keine Verlängerung.
- RFS wird gemäß § 20k BKAG-E gelöscht, keine RFS mehr auf dem Zielrechner.
- Aber: Lageabhängig besteht ein dringender Bedarf für eine (erneute) Onlinedurchsuchung bei der ZP.
- Das geeignete Tool (RFS) steht weiter zur Verfügung.
- Hier Besonderheit gegenüber den o. g. Fallkonstellationen 1 und 2: Aufbringungsmöglichkeit bietet sich durch unmittelbaren Zugriff auf den Zielrechner!

Es geht um Lebenssachverhalte wie z. B. die Reparatur eines PC oder den Kneipenbesuch, die Autobahnraststätte o. ä., die zum kurzzeitigen Zugriff auf das Gerät zwecks Aufbringens genutzt werden sollen, ohne den www-Weg zu nutzen. Wie in den beiden zuvor genannten Fällen liegt eine individuelle RFS bereits vor. Somit besteht, ohne eine Wohnung zu betreten, die Möglichkeit des unverzüglichen Aufbringens der Software durch einen Memorystick oder in anderer Weise bei taktischer Gelegenheit des physikalischen Zugriffs auf das informationstechnische System der Zielperson. Die Zugriffsmöglichkeit kann sich dabei lageabhängig ergeben, wenn sich z. B. der Rechner der Zielperson in einer Servicewerkstatt befindet oder z. B. das Notebook von der Zielperson im geparkten Kfz belassen wird und daher eine Gelegenheit zum Aufspielen der RFS besteht.

4. Fallkonstellation

- Software wird nach § 20l Abs. 2 BKAG-E (Quellen-TKÜ) erfolgreich auf das Zielsystem aufgespielt. Damit ist die Konfiguration des Zielsystems auch für die Aufbringung des Tools für die Online-DS bekannt.
- In den anschließenden Ermittlungen wird erkennbar, dass auch eine Online-DS auf dem Zielsystem erforderlich wird.
- Eilanordnung erforderlich.

Das BKA führt im Rahmen der Gefahrenabwehr eine Quellen-TKÜ gemäß § 20l Abs. 2 BKAG-E durch. Diese Maßnahme wird bei besonderen Gefahrenlagen „live“, das heißt 24 Stunden am Tag, abgehört. Durch überwachte Gesprächsinhalte und die Feststellung von starkem Datenverkehr, der offensichtlich durch Downloads ausgelöst ist, wird eine sofortige ODS notwendig, da der Verdacht besteht, dass sich der Täter eine Anleitung zum Bau eines Sprengsatzes oder Ähnliches herunter lädt. Das Aufspielen einer individuellen Remote Forensic Software ist in Stundenfrist möglich, da durch die bestehende Quellen-TKÜ die Konfiguration des Zielsystems bereits bekannt ist.

Besonderheit in dieser Konstellation:

Die Ermittlungsschritte sind (s. o. schon im Ausgangsfall)

- a) konventionelle TKÜ
- b) Quellen-TKÜ
- c) Onlinedurchsuchung.

Da hier bereits eine Quellen-TKÜ läuft und damit auch die Konfiguration des Zielsystems bekannt ist, kann bei Vorliegen der Voraussetzungen des § 20k BKAG umgehend das ODS-Tool nachgeladen werden. Angesichts der im Ausgangsfall hier in wenigen Stunden ab Kenntniserlangung in der Nacht von Samstag auf einen Sonntag angenommenen Übermittlung einer E-Mail mit verschlüsseltem Inhalt (ist einer Quellen-TKÜ nicht zugänglich, s. o. im Ausgangsfall) darf nicht auf eine richterliche Entscheidung zur ODS erst am nächsten Montag zugewartet werden. Maßnahme kann unverzüglich realisiert werden, Eilfallbefugnis erforderlich.

Darüber hinaus geben die Koalitionsfraktionen folgende weitere Erklärung ab:

„Aus der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 103, 142, 153; in Bezug genommen im Urteil zur Online-Entscheidung vom 27. Februar 2008, dort Rdnr. 261) ergeben sich folgende verfassungsrechtliche Vorgaben für die Zulässigkeit einer nichtrichterlichen Anordnung einer grundrechtseingreifenden Maßnahme bei „Gefahr im Verzug“.

Die nichtrichterliche Anordnung bei „Gefahr im Verzug“ enthält eine Ausnahme vom Grundsatz der richterlichen Entscheidung. Vor allem wegen der grundrechtssichernden Schutzfunktion des Richtervorbehalts ist „Gefahr im Verzug“ deshalb eng auszulegen. Die betroffenen Behörden und die Gerichtsorganisation haben danach im Rahmen des Möglichen sicherzustellen, dass in der Masse der Alltagsfälle die in der Verfassung vorgesehene „Verteilung der Gewichte“, nämlich die Regelzuständigkeit des Richters, gewahrt bleibt. Hiernach muss „Gefahr im Verzug“ mit Tatsachen begründet werden, die auf den Einzelfall bezogen sind. Es muss regelmäßig versucht werden, eine Anordnung des instanzuell und funktionell zuständigen Richters zu erlangen, bevor die Eingriffsmaßnahme ergriffen wird. Nur in Ausnahmesituationen, wenn schon die zeitliche Verzögerung wegen eines solchen Versuchs den Erfolg der Maßnahme gefährden würde, darf die Behörde selbst die Anordnung wegen Gefahr im Verzug treffen, ohne sich zuvor um eine richterliche Entscheidung bemüht zu haben. Die Annahme von „Gefahr im Verzug“ kann insbesondere nicht allein mit dem abstrakten Hinweis begründet werden, eine richterliche Entscheidung sei gewöhnlicherweise zu einem bestimmten Zeitpunkt oder innerhalb einer bestimmten Zeitspanne nicht zu erlangen. Dem korrespondiert die verfassungsrechtliche Verpflichtung der Gerichte, die Erreichbarkeit eines Ermittlungsrichters, auch durch die Einrichtung eines Eil- oder Notdienstes, zu sichern.

Des Weiteren weisen wir daraufhin, dass die Benachrichtigungsregelungen in § 20w Absatz 5 BKAG-E den zum 1. Januar 2008 neu gefassten Benachrichtigungsregelungen in der Strafprozessordnung (§ 101 StPO) nachgebildet sind.“

II. Zur Begründung

1. Zur Begründung des Gesetzentwurfs wird allgemein auf Drucksachen 16/9588 und 16/10121 hingewiesen. Die auf Grundlage des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 16(4)505 vom Innenausschuss vorgenommenen Änderungen begründen sich wie folgt:

Zu Nummer 1

Durch die Änderung wird im Rahmen von Maßnahmen nach § 20c eine Ausnahme von der grundsätzlich nach § 20c Abs. 3 Satz 2 bestehenden Auskunftspflicht auch von zeugnisverweigerungsberechtigten Personen zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person eingeführt. Für Zugehörige der drei benannten Berufsgruppen besteht im Rahmen des jeweiligen Rechts zur Zeugnisverweigerung ein ausnahmsloses Recht zur Verweigerung der Auskunft. Diese Änderung entspricht der Systematik in der allgemeinen Regelung zum Schutz zeugnisverweigerungsberechtigter Personen aus § 20u.

Durch die Änderung wird die Möglichkeit einer Eilanordnung durch den Präsidenten des Bundeskriminalamtes oder seines Vertreters gestrichen. Es ist damit ausnahmslos eine richterliche Anordnung erforderlich.

Durch die Änderung ist das im Rahmen der Maßnahme des verdeckten Eingriffs in informationstechnische Systeme eingesetzte Mittel allein nach dem Stand der Technik, und nicht wie bisher vorgesehen, auch nach dem Stand der Wissenschaft gegen unbefugte Nutzung zu schützen.

Durch die Änderung sind die im Rahmen der Maßnahme des verdeckten Eingriffs in informationstechnische Systeme kopierten Daten allein nach dem Stand der Technik, und nicht wie bisher vorgesehen, auch nach dem Stand der Wissenschaft gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

Durch die Änderung von Satz 3 wird der Kreis der Personen, die die mittels der Onlinedurchsuchung erhobenen Daten auf Kernbereichsrelevanz zu prüfen haben, um den Datenschutzbeauftragten des BKA erweitert. Der Datenschutzbeauftragte ist in Anlehnung an § 4f Abs. 3 BDSG bei der Ausübung dieser Aufgabe weisungsfrei und darf nicht benachteiligt werden. Zusammen mit der Änderung des neuen Satzes 6, wonach bei Zweifeln eines der Beteiligten oder bei Uneinigkeit zwischen den Beteiligten in Bezug auf die Kernbereichsrelevanz die Daten entweder zu löschen oder unverzüglich dem anordnenden Gericht zur Entscheidung vorzulegen sind, ist damit ein geeignetes Verfahren vorgesehen, das den Belangen des Betroffenen hinreichend Rechnung trägt und den verfassungsrechtlichen Anforderungen an die Ausgestaltung des Kernbereichsschutzes genügt (vgl. BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07 Absatznummer 282 und 283).

Es handelt sich um die Bereinigung eines Redaktionsverehens.

Absatz 5 wird insgesamt neu gefasst. Satz 1 Nr. 2 wird insoweit ergänzt, als nunmehr auch eine Übermittlung zur

Verhütung der in § 129a Abs. 1 und 2 aufgelisteten Straftaten ermöglicht wird. Satz 2 stellt klar, dass abweichend von § 20a Abs. 2 die für die Übermittlung erforderliche konkrete Gefahr keinen Bezug zum internationalen Terrorismus haben muss. Satz 3 regelt nunmehr die Übermittlung personenbezogener Daten an die Verfassungsschutzbehörden des Bundes und der Länder sowie den Militärischen Abschirmdienst. Satz 4 regelt nunmehr die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst. Die Sätze 3 und 4 entsprechen § 23d Abs. 4 und 5 des Zollfahndungsdienstgesetzes. Die Übermittlung personenbezogener Daten an die genannten Behörden ist danach nur zulässig, wenn die Erforderlichkeit der Übermittlung durch tatsächliche Anhaltspunkte bzw. bestimmte Tatsachen belegt ist. Zudem sind die Übermittlungszwecke eng eingegrenzt. Die Datenübermittlung wird damit im Vergleich zur im Entwurf vorgesehenen Regelung eingeschränkt. Dies trägt dem auch in der Rechtsprechung des Bundesverfassungsgerichts enthaltenen Gedanken Rechnung, dass die Schwere des jeweiligen Grundrechtseingriffs bei der Datenerhebung mit den jeweiligen Übermittlungsmöglichkeiten korrelieren muss.

Zu Nummer 2

Die vorgesehene Evaluierung dient dazu, die Auswirkungen von denjenigen Teilen des neuen Unterabschnitts zu überprüfen, zu denen bisher mangels Regelungsvorbildern bzw. mangels Regelungsvorbildern in Bundesgesetzen keine Erfahrungswerte vorliegen. Im Rahmen der Evaluierung von § 4a BKAG soll das Funktionieren der Zusammenarbeit von Bund und Ländern untersucht werden. Die Evaluierung der Aufgabennorm des § 4a BKAG soll hingegen nicht dazu führen, dass alle zur Erfüllung dieser Aufgabe eingesetzten oder einsetzbaren Befugnisse betrachtet werden. Dies zeigt schon, dass die Evaluierung der sog. Onlinedurchsuchung nach § 20k BKAG als eine dieser Befugnisse ausdrücklich vorgesehen ist, während andere Befugnisnormen nicht genannt werden.

Zu Nummer 3

Mit der Änderung wird die Befugnis zum verdeckten Eingriff in informationstechnische Systeme bis zum 31. Dezember 2020 befristet.

2. Die **Fraktion der CDU/CSU** betont, der international agierende und organisierte Terrorismus mache eine zentrale Steuerung der Gefahrenabwehr in diesem Bereich erforderlich. Die Koalitionsfraktionen hätten den ersten Entwurf des Gesetzes im Lichte der Sachverständigenanhörung nochmals verbessert. Neben einer aufwändigen Regelung des Kernbereichsschutzes, die in allen Zweifelsfällen die Einschaltung eines Richters vorsehe, sei nunmehr für wichtige Neuerungen eine Evaluierung nach fünf Jahren vorgesehen. Auch wenn man für die Onlinedurchsuchung jetzt eine Befristung geregelt habe, sei angesichts der rasanten technischen Entwicklung im kriminellen und terroristischen Umfeld allerdings kaum damit zu rechnen, dass die dringend erforderliche Vorschrift dann tatsächlich außer Kraft trete. Insgesamt werde das Gesetz eine Lücke im Sicherheitssystem der Bundesrepublik Deutschland schließen und die Sicherheitsstandards weiter optimieren.

Die **Fraktion der SPD** hebt den großen Nutzen der Anhörung für die Verbesserungen hervor, die der Änderungsantrag bringe. Gerade die Regelung, dass nunmehr auch der Datenschutzbeauftragte des BKA in die Prüfung auf kernbereichsrelevante Inhalte einbezogen werde, sei vorbildlich. Das BKA werde mit der Neuregelung keinesfalls ein deutsches „FBI“. Die Erklärung zu den Eilfallregelungen stelle klar, dass richterliche Notdienste eingerichtet werden müssten und dass auch tatsächlich versucht werden müsse, einen Richter zu erreichen. Die Evaluierung von Vorschriften nach fünf Jahren sei ein wichtiger Schritt – auch in Hinblick darauf, ob sich die Regelung für die Zusammenarbeit zwischen BKA und Landeskriminalämtern bewähre. Die Regelung beim Kernbereichsschutz sei sehr sensibel, bei den Zeugnisverweigerungsrechten entspreche sie dem Standard verschiedener Gesetze. Es gebe kein besseres, rechtsstaatlich vorbildlicheres Polizeigesetz in den Ländern.

Die **Fraktion der FDP** lehnt das Gesetz insgesamt ab und rügt diverse Einzelregelungen des Entwurfs. So sei eine schlechtere Abstimmung zwischen BKA und Landeskriminalämtern zu befürchten, die Definitionen von internationalem Terrorismus und von Kontakt- und Begleitpersonen seien unklar, die Abgrenzung der Tätigkeiten von BKA und Generalbundesanwaltschaft sei unklar, der Kernbereichsschutz werde weiterhin nur unzureichend gewährleistet, die Eilfallregelungen seien bedenklich und die Onlinedurchsuchung werde keine gerichtlich verwertbaren Ergebnisse liefern. Es reiche nicht aus, das Bundesverfassungsgericht wörtlich zu zitieren, wenn man den Sinngehalt der Entscheidungen nicht berücksichtige. Auch die Befristung bis 2020 schließlich sei deutlich zu lang und die Berufsheimnisträger seien nach wie vor unzureichend geschützt. Dieses Gesetz sei in dieser Eingriffstiefe beispiellos.

Die **Fraktion DIE LINKE** erklärt, auch sie werde das Gesetz ablehnen, und kritisiert, dass der Änderungsantrag nur marginale Veränderungen bringe und nichts Maßgebliches aus der Anhörung berücksichtige. Das Gesetz enthalte schwammige Begriffsdefinitionen, etwa bei internationalem Terrorismus und dem Gefährderbegriff, und räume dem BKA umfangreiche neue Befugnisse ein, die weitgehende Eingriffe in Grundrechte ermöglichen, die noch vor einigen Jahren undenkbar gewesen wären. Mit den Mitteln von Rasterfahndung, Späh- und Lauschangriffen und der Ermittlung im Vorfeldbereich ähnele das BKA mehr einem Geheimdienst als einer Polizei. Besonders bedenklich seien auch die Regelungen der Einschränkungen der Zeugnisverweigerungsrechte von Anwälten und Journalisten.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** hält das Gesetz insgesamt für nicht erforderlich. Mit der Machtkonzentration beim BKA entstehe ein „deutsches FBI“, das parlamentarisch kaum kontrolliert werden könne. Der Richtervorbehalt sei nur lückenhaft geregelt, das BKA werde von der Generalbundesanwaltschaft abgekoppelt, die in diesem Bereich praktisch nichts mehr zu sagen habe. Bei den Eilfallregelungen müsse man sich fragen, warum die Klarstellung nicht im Gesetz enthalten sei, sondern in einem Anschreiben, und warum nicht die organisatorischen Voraussetzungen für eine ständige Erreichbarkeit von Richtern geschaffen würden. Bedenklich sei es, die Auskunftspflicht bei Anwälten beizubehalten und BKA-Beamte mit eigenem Ermittlungsinteresse mit der Kontrolle auf kernbereichsrelevante Inhalte hin zu betrauen. Die Beteiligung eines hauseigenen Datenschutzbeauftragten heile diesen Grundfehler nicht. Die geplante Teilevaluierung des Gesetzes reiche nicht aus, die Befristung bis 2020 sei zu lang und die Zentralisierung der Sicherheitsarchitektur sei eine Lösung von gestern.

Berlin, den 10. November 2008

Helmut Brandt
Berichterstatter

Michael Hartmann (Wackernheim)
Berichterstatter

Frank Hofmann (Volkach)
Berichterstatter

Gisela Piltz
Berichterstatterin

Ulla Jelpke
Berichterstatterin

Wolfgang Wieland
Berichterstatter

