Dr. Hans-Peter Uhl
Mitglied des Deutschen Bundestages
Innenpolitischer Sprecher der
CDU/CSU-Bundestagsfraktion

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)505

Dr. Dieter Wiefelspütz
Mitglied des Deutschen Bundestages
Innenpolitischer Sprecher der
SPD-Bundestagsfraktion

05. November 2008

Vorsitzender des Innenausschusses
Herrn
Sebastian Edathy, MdB

Sehr geehrter Herr Vorsitzender,

zu dem Gesetzentwurf der Fraktionen der CDU/CSU und SPD sowie der Bundesregierung

Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt
Drucksache 16/9588, 16/10121

stellen wir den beigefügten Änderungsantrag.

Wir bitten, die beigefügten Beispielfälle zur Erforderlichkeit der Eilfallregelung bei der Online-Durchsuchung (§ 20k BKAG-E) als Ausschussdrucksache den Beratungen im Innenausschuss zu Grunde zu legen, in den Bericht aufzunehmen und dem Protokoll beizufügen.

Darüber hinaus bitten wir folgende Erklärung in den Bericht aufzunehmen:

„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 instanziell 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.

Desweiteren weisen wir daraufhin, dass die Benachrichtigungsregelungen in § 20 w Absatz 5 BKAG-E den zum 01. Januar 2008 neu gefassten Benachrichtigungsregelungen in der Strafprozessordnung (§ 101 StPO) nachgebildet sind.“

Mit freundlichen Grüßen

Hans-Peter Uhl

Dieter Wiefelspütz

05.11.2008

Änderungsantrag der Fraktionen CDU/CSU und SPD
im 4. Ausschuss (Innenausschuss) des Deutschen Bundestages

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

Der Bundestag wolle beschließen,
den Gesetzentwurf auf Drucksachen 16/9588 sowie 16/10121 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

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

   a) § 20c Abs. 3 wird wie folgt gefasst:

      Nach Satz 2 wird folgender Satz eingefügt:
      „Eine in § 53 Abs. 1 Satz 1 Nr. 1, 2 oder 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 gestrichen.

   c) § 20k Abs. 2 Satz 2 wird wie folgt gefasst:
      „Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen."

   d) § 20k Abs. 2 Satz 3 wird wie folgt gefasst:
      „Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen."

   e) § 20k Abs. 7 wird wie folgt gefasst:

      Satz 3 wird wie folgt gefasst und es wird danach folgender Satz eingefügt:
      „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. Der Datenschutzbeauftragte

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

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.“

f) § 20t Abs. 1 Satz 1 Nr. 1 wird wie folgt gefasst:

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

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

„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 § 4 a 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 §§ 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 §§ 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**,** § 20 j und § 20k sind 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 31.12.2020 außer Kraft.“

Begründung:

Zu Nummer 1

a) 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.

b) 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.

c) 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.

d) 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.

e) Durch die Änderung von Satz 3 wird der Kreis der Personen, die die mittels der Online-Durchsuchung 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 Kernbereichschutzes genügt (vgl. BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07, 1 BvR 595/07 Absatznr. 282 und 283).

f) Es handelt sich um die Bereinigung eines Redaktionsversehens.

g) Absatz 5 wird insgesamt neu gefasst. Satz 1 Nummer 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 Evaluation der sog. Online-Durchsuchung 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 31.12.2020 befristet.

§ 20 k BKAG-E (Online-Durchsuchung)

Konstellationen zum Bedarf der Normierung einer Eilfallregelung bei § 20k BKAG-E

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 Online-Durchsuchung wäre hier zielführend gewesen, die Konstellation einer Eilfallregelung kann seitens 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 §§ 129a, b StGB liegen bislang keine ausreichenden Hinweise vor.

Nach Erkenntnissen des britischen Geheimdienstes werden Kontakte ausschließlich per 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 Anschlagspläne 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 Anschlagspläne 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 Anschlagsplänen auf dem Computersystem von X ebenfalls ausschließlich verschlüsselt abgespeichert sind (eine Beschlagnahme des Computersystems würde daher zu keinen Erkenntnissen führen).

Eine TKÜ-Maßnahme ist alleine nicht zielführend: Da X nur kryptiert kommuniziert, läuft schon eine "konventionelle" TKÜ ins Leere. Eine Quellen-TKÜ nach § 20 l II 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 Online-Durchsuchung dann zugegriffen werden, wenn sie von der Zielperson 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 Online-Durchsuchung 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 Anschlagsziel und -zeitpunkt sowie die geplante Vorgehensweise erlangt werden. Der konkrete Zeitpunkt des "Tag X" für den geplanten Anschlag ist noch nicht abzusehen, auch wo der Anschlag begangen werden soll, ist den Ermittlern noch nicht bekannt.

1. Fallkonstellation:

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

Die RFS wurde bereits für eine zurückliegende § 20k-BKAG-E-Maßnahme entwickelt und bei der Zielperson eingesetzt. Nach Beendigung der Maßnahme und Löschung der RFS auf dem Zielsystem ist aufgrund einer Lageänderung bzw. neuer Lageerkenntnisse der Bedarf nach einer weiteren Online-Durchsuchungsmaßnahme 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; 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: 3 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 Online-Durchsuchung vorbereitet**
- **Maßnahme konnte jedoch aus taktischen Gründen nicht realisiert werden.**
- **Richterliche Anordnung läuft nach 3 Monaten aus.**
- **Keine RFS auf dem Zielrechner.**
- **Später wird eine weitere Online-Durchsuchung erforderlich und Realisierungsmöglichkeit (günstiges Zeitfenster) bietet sich**

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 fertig gestellt („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 „Online-Zeit“

erwarten lässt und eine richterliche Entscheidung nicht zeitnah zu erlangen ist. Das RFS-Tool ist bereits einsatzfähig.

3. Fallkonstellation:

- **RFS wurde bei einer angeordneten Online-Durchsuchung vorbereitet und**
  - **Maßnahme konnte aus taktischen Gründen nicht realisiert werden (s. Fallkonstellation 2) <u>oder</u>**
  - **Maßnahme wurde durchgeführt (s. Fallkonstellation 1)**
- **Maßnahme wurde beendet.**
- **Richterlicher Anordnungszeitraum läuft ab, keine Verlängerung**
- **RFS wird gem. § 20k BKAG-E gelöscht, keine RFS mehr auf dem Zielrechner**
- **Aber: Lageabhängig besteht ein dringender Bedarf für eine (erneute) Online-Durchsuchung bei der ZP.**
- **Das geeignete Tool (RFS) steht weiter zur Verfügung.**
- **hier Besonderheit ggü. 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 einem Memory-Stick 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 § 20 l 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.) Online-Durchsuchung.

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.